

**reference
guide**

hp StorageWorks FCIP/iSCSI Storage Router 2122-2 Command Line Interface

Product Version: 1.0A

Product Version: Third Edition (December 2003)

Part Number: 306001-002

This Command Line Interface (CLI) Reference Guide provides information to help you configure the Storage Router using the CLI.



© Copyright 2003 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice.

All other product names mentioned herein may be trademarks of their respective companies.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

HP StorageWorks iSCSI Storage Router 2122-2 Command Line Interface Reference Guide
Third Edition (December 2003)
Part Number: 306001-002

contents

Conventions	xii
Rack Stability	xiv
Getting Help	xv
1 Introduction	
Definitions	1
Reserved Words	3
Basic Monitor Commands	3
Administrative Commands	4
2 Authentication, Authorization, and Accounting Commands	
aaa authentication enable	7
aaa authentication iscsi	9
aaa authentication login	12
aaa generate password	14
aaa group server radius	15
aaa group server tacacs+	16
aaa new-model	17
aaa test authentication	18
aaa test authentication cancel	19
debug aaa	20
ip radius source-interface	21
ip tacacs source-interface	22
radius-server deadtime	23
radius-server host	24
radius-server key	27
radius-server retransmit	28
radius-server timeout	29
scsirouter authentication	30
show aaa	31

tacacs-server host	34
tacacs-server key	36
tacacs-server timeout	37
username password	38

3 Administrative Commands

admin contactinfo	42
admin password	43
delete script	45
enable	46
exit	46
halt	48
help	49
hostname	50
logout	51
monitor password	52
read	53
reboot	56
show admin	57
show buffers	58
show cli	64
show cpu	65
show crash	66
show diagnostics	67
show memory	68
show modules	69
show restrict	71
show script	72
show sessions	74
show stack	75
show system	77
show task	79
show tech-support	82

4 CDP Commands

cdp enable	86
cdp holdtime	87
cdp interface	88
cdp timer	89

show cdp	90
show cdp entry	91
show cdp interface	92
show cdp neighbors	94
show cdp traffic	98
5 Clock Commands	
clock set	102
clock timezone	103
ntp peer	104
show clock	105
6 Configuration Commands	
delete savedconfig	108
restore aaa	109
restore accesslist	110
restore all	111
restore scsirouter	113
restore system	114
restore vlan	116
save aaa	117
save accesslist	119
save all	120
save fc-server	122
save scsirouter	123
save system	124
save vlan	125
show boot	127
show bootconfig	128
show runningconfig	133
show savedconfig	135
7 Fibre Channel Port Commands	
interface fci? mode	137
interface fc? topology	140
show debug fc?	141
show debug interface fc?	143
show devices	145
show hosts	148
show interface	150

8 Fibre Channel Server Commands

clear counters fc-server	158
delete fc-server	159
fc-server autoconfig	160
scsirouter client authenticate	161
fc-server description	163
fc-server enable	164
fc-server server	165
fc-server serverif	166
show debug fc-server	168
show fc-server	170

9 HA Commands

clear scsirouter failover	176
failover scsirouter	177
interface ha	178
scsirouter failover	180
scsirouter password	182
scsirouter primary	183
show cluster	185
show ha	187

10 IP Commands

clear counters fcip	194
clear counters interface	195
clear scsirouter primary	196
debug ip rip	197
debug isns	199
debug scsirouter iscsitrace	201
interface ge?	203
interface ge? ip-address	205
interface ha ip-address	206
interface mgmt	207
interface mgmt ip-address	209
ip default-gateway	210
ip domain-name	211
ip name-server	212
ip route	213
isns enable	215

isns refresh	217
ping	218
restrict console	219
restrict	220
scsirouter serverif	224
show debug isns	226
show debug interface ge?	228
show ip	230
show isns	232
show route	237
11 Logging Commands	
clear log	240
logging syslog	241
logging	242
logging on	243
show logging	244
12 SCSI Commands	
scsirouter lun reset	248
scsirouter reserveproxy	249
scsirouter target accesslist	250
scsirouter target description	252
scsirouter target {enabled disabled}	253
scsirouter target {serial lunwwn wwpn} #?	255
scsirouter target lun serial	258
scsirouter target lun lunwwn	260
scsirouter target lun targetid	262
scsirouter target lun wwpn lun	263
scsirouter target profile	265
scsirouter target wwpn	266
13 SCSI Router Commands	
accesslist	269
accesslist description	272
clear counters scsirouter	273
clear static	274
debug fcip	276
debug scsirouter	278

debug scsirouter target	279
delete accesslist.	280
delete fcip	283
delete scsirouter	284
fcip	287
fcip destination config	289
fcip destination tcpclient.	293
fcip destination tcpserver	295
fcip enable.	298
fcip networkif	299
restore fcip	303
save fcip	305
scsirouter cdbretrycount	306
scsirouter.	308
scsirouter authentication	309
scsirouter client authenticate.	310
scsirouter description	311
scsirouter enable	312
scsirouter failover	313
scsirouter lun reset	316
scsirouter password.	318
scsirouter primary	321
scsirouter serverif	323
scsirouter slp enable	327
Defaults.	327
scsirouter target accesslist.	329
scsirouter target crc.	333
scsirouter target description	336
scsirouter target enable	338
scsirouter target {lunid serial wwpn} #?.	342
scsirouter target lun lunid	346
scsirouter target lun serial.	349
scsirouter target maxcmdqueuedepth	356
scsirouter target trespass.	358
scsirouter username	360
setup fcip.	362
show accesslist	365
show debug scsirouter.	367

show debug fcip	373
show scsirouter	375
slp findattrs	385
slp findsrvtypes	389
static iscsibinding interface autolearn	390
static iscsibinding interface index	392
14 SNMP Commands	
show snmp	396
snmp-server	397
15 Software Management Commands	
copy http	402
copy tftp	403
delete software version	405
download software	406
show software version	408
show version	409
software http url	410
software http username	411
software proxy	412
software proxy url	413
software proxy username	415
software tftp	416
software version	417
verify software	419
16 Commands	
show vlan	424
show vtp	425
vlan	427
vtp domain	428
vtp mode	430
17 Wizard Commands	
clear conf	434
clear conf all	437
clear conf system	438
scsirouter username	439

setup	440
setup access.....	443
setup cluster	446
setup mgmt	450
setup netmgmt.....	452
setup scsi.....	453
setup time	455
A Regulatory Compliance Notices	
Regulatory Compliance Identification Numbers	457
Federal Communications Commission Notice.....	457
Mouse Compliance Statement	460
Canadian Notice (Avis Canadien)	460
European Union Notice	461
Japanese Notice	461
Taiwanese Notice	462
Laser Device.....	462
B Electrostatic Discharge	
Grounding Methods	466

about this guide

This Command Line Interface (CLI) Reference Guide provides information to help you configure the Storage Router using the CLI.

The CLI commands are divided into the following categories:

- Chapter 2 — “AAA Commands”
- Chapter 3 — “Administrative Commands”
- Chapter 4 — “CDP Commands”
- Chapter 5 — “Clock Commands”
- Chapter 6 — “Configuration Commands”
- Chapter 7 — “Fibre Channel Port Commands”
- Chapter 8 — “Fibre Channel Server Commands”
- Chapter 9 — “HA Commands”
- Chapter 10 — “IP Commands”
- Chapter 11 — “Logging Commands”
- Chapter 12 — “SCSI Commands”
- Chapter 13 — “SCSI Router Commands”
- Chapter 14 — “Software Management Commands”
- Chapter 16 — “VLAN Commands”
- Chapter 17 — “Wizard Commands”

About this Guide topics include:

- [Conventions](#), page xii
- [Rack Stability](#), page xiv
- [Getting Help](#), page xv

Conventions

Conventions consist of the following:

- [Document Conventions](#)
- [Text Symbols](#)
- [Equipment Symbols](#)

Document Conventions

The document conventions included in [Table 1](#) apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Figure 1
Key and field names, menu items, buttons, and dialog box titles	Bold
File names, application names, and text emphasis	<i>Italics</i>
User input, command and directory names, and system responses (output and messages)	Monospace font COMMAND NAMES are uppercase monospace font unless they are case sensitive
Variables	<i><monospace, italic font></i>
Website addresses	Underlined sans serif font text: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.



Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings.



Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of injury from electrical shock hazards, do not open this enclosure.



Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.



Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personal and equipment.



WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
 - The full weight of the rack rests on the leveling jacks.
 - In single rack installations, the stabilizing feet are attached to the rack.
 - In multiple rack installations, the racks are coupled.
 - Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.
-

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our website: <http://www.hp.com>.

HP Technical Support

In North America, call technical support at 1-800-652-6672, available 24 hours a day, 7 days a week.

Note: For continuous quality improvement, calls may be recorded or monitored.

Outside North America, call technical support at the nearest location. Telephone numbers for worldwide technical support are listed on the HP website under support: <http://www.hp.com/support>.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Website

The HP website has the latest information on this product, as well as the latest drivers. Access storage at: <http://www.hp.com>. From this website, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP website for locations and telephone numbers:
<http://www.hp.com>.

Introduction

1

This document describes the Command Line Interface (CLI) for the HP StorageWorks Storage Router SR 2122. The Storage Router provides access to the CLI over the serial port or either of the two management Ethernet ports.

This introduction chapter includes the following topics:

- [Definitions](#), page 1
- [Special Keys](#), page 2
- [Reserved Words](#), page 3
- [Basic Monitor Commands](#), page 3
- [Administrative Commands](#), page 4

Definitions

This section defines words, acronyms, and actions, including:

- <A.B.C.D>/Bits — A.B.C.D refers to the network or host Ipv4 specification. “Bits” refers to the netmask in the CIDR style, meaning the number of bits in the netmask counting from the most significant (left) side.
- HA — High Availability operational functions
- MAC — Media Access Control
- FC — Fibre Channel
- GbE — Gigabit Ethernet
- `bootconfig` — Properties stored in files contained in the directory `/ata0/conf` or one of its subdirectories. These values are stored on disk in the `/ata0/conf` directory are used to initialize applications when the box is rebooted.

- `runningconfig` — Uses the same properties as `bootconfig` but the values are read from memory.
- `savedconfig` — One or more files saved in the `savedconfig` directory that contain a snapshot of these property values (as read-from memory) at a point in time. These files have a unique name that is used to identify them.

Special Keys

Like many other command-line shells, a **tab** key completes the current word that is being typed up to a point of ambiguity. A question-mark “?” will list all of the options available at that point in the command line, along with a brief description of the meaning of the options. Any individual word may be truncated at any point after it is unique. This, in combination with **tab** completion, allows long command lines to be entered rapidly with very few keystrokes. [Table 2](#) describes special keys that can be used while typing in a CLI command:

Table 2: Special Keys

Key	Function
?	Lists choices
Backspace, Delete	Deletes character backward
Tab	Completes current word
Ctrl-A	Goes to beginning of line
Ctrl-B or Arrow Left	Goes backward one character
Ctrl-D	Deletes character
Ctrl-E	Goes to end of line
Ctrl-F or Arrow Right	Goes forward one character
Ctrl-K	Deletes from current position to end of line
Ctrl-N or Arrow Down	Goes to next line in history buffer
Ctrl-T	Transposes current character and previous character
Ctrl-P or Arrow Up	Goes to previous line in history buffer
Ctrl-U	Deletes line
Ctrl-W	Deletes previous word

Reserved Words

Reserved words are not case-insensitive; So “aLL,” ALL,” or “All” is considered to match the reserved word “all.” [Table 3](#) list the reserved words.

Table 3: Reserved words

Reserved Words			
accesslist	disabled	loopid	restore
acl	enable	looppref	scsirouter
all	enabled	lunid	scsitrace
authenticate	failover	none	server
Canonical	force	passthru	servers
bus1	ha	password	serverif
bus2	import	proxy	snmp
clear	iprouter	ptp	table
client	iptan	ptppref	targetid
default	iscsi	rediscover	tfestatus
deviceif	loglevel	reserve	username
disable	loop	reset	wwpn

Basic Monitor Commands

The CLI supports the following basic monitor commands:

Table 4: Basic Monitor Commands

Commands	Descriptions
clear	Clears statistical counters, configurations, and log files
enable	Enters the "Administrator" (Privileged) level
help	Displays help on top-level commands, including special key descriptions
logging	Enables logging to the console, for a storage router, or remotely
ping	Verifies communication with another system or storage router in the network
show	Displays configuration, statistics, and operational data

Administrative Commands

The CLI supports the following administrative commands:

Table 5: Administrative Commands

Commands	Descriptions
aaa	Enables AAA access control model, methods, and testing
accesslist	Configures access lists which control access to storage routers
admin	Sets administrative contact information and password
cdp	Enables and configures CDP information
clear	Clears statistical counters, configurations, and log files
clock	Sets date and time information
copy	Imports or exports a saved configuration or script file
debug	Enables trace facilities for debugging SCSI routing and AAA services
delete	Deletes selected entities that were created or added
download	Downloads new software for the SR 2122
exit	Leaves the "Administrator" level and goes back to the "Monitor" level
failover	Stops and then starts SCSI Router running on another storage router
ha	Resets import pending flag for a storage router in a cluster
help	Displays help on top level commands including special key descriptions
hostname	Sets the system name of the storage router
interface	Sets various operational parameters for fc1, ge2, ha, or mgmt
ip	Configures IP interface parameters like the default gateway, domain name, and static route
logging	Enables logging to the console, SR 2122 log file, or remotely
logout	Terminates the session
monitor	Sets the monitor password
no	Disables or clears named entities
ntp	Sets NTP server name

Table 5: Administrative Commands (Continued)

Commands	Descriptions
ping	Verifies communications with another system or storage router in the network
radius-server	Sets the RADIUS server host, key, number of resends, and timeout parameter
read	Reads and executes CLI commands from a file
reboot	Shuts down and reboots the SR 2122
restore	Installs configuration data from an imported file or previously saved file
restrict	Enables password checking and access to interfaces like HTTP
save	Saves all configurations or configurations for named entities
scsirouter	Sets various SCSI router parameters
setup	Runs various configuration wizards
show	Displays configuration, statistics, and operational data
snmp-server	Enables SNMP and sets read and write access to the storage router network
software	Configures download parameters like location, passwords, proxy server, and tftp server
tacacs-server	Sets the TACACS+ server host, key, and timeout parameters
username	Builds a local user name database to be used by AAA authentication
verify	Verifies SR 2122 software
vlan	Configures a VLAN for cluster-wide configurations
vtp	Assigns a VTP domain name and mode to the storage router

Authentication, Authorization, and Accounting Commands

2

This chapter describes the CLI commands related to AAA. The no form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

aaa authentication enable

To configure an enable authentication method list for users requesting admin access to a storage router, use the `aaa authentication enable` command. To delete an enable authentication method list, use the no form of this command.

Syntax

```
aaa authentication enable default method1 [method2...]  
no aaa authentication enable default
```

Table 6: Syntax Description

default	Makes the listed authentication methods that follow this argument the default list.
method1 [method2...]	At least one of the methods described in Table Note: .

Defaults

If the default enable authentication list is not configured, only the admin password is selected. This has the same effect as the following command:

```
aaa authentication enable default admin
```

Command Modes

Administrator.

Usage Guidelines

Enable authentication uses AAA authentication services to provide authentication of user requesting admin privilege via the `enable` command.

AAA uses each service in the order listed in the `enable default` authentication list, until authentication succeeds or fails. When using a RADIUS or TACACS+ server, a user name of “\$enable\$” will be used. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA uses the next service in the list for authentication.

Use the `show runningconfig` command to display the current list of authentication services.

Note: In [Table 7](#), the group RADIUS and group TACACS+ methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the `RADIUS-server host` and `TACACS+-server host` commands to configure the host servers.

Table 7: AAA Authentication Enable Methods

Keyword	Description
<code>enable</code>	Uses the admin password, as specified with the <code>admin password</code> command.
<code>group radius</code>	Uses the list of all RADIUS servers for authentication.
<code>group tacacs+</code>	Uses the list of all TACACS+ servers for authentication.
<code>group groupname</code>	Uses the server group <code>groupname</code>
<code>monitor</code>	Uses the monitor password, as specified with the <code>monitor password</code> command.
<code>none</code>	Uses no authentication.

Examples

The following example creates a new AAA authentication list. When enable authentication is required, AAA first tries to contact a TACACS+ server. If no server is found, the *admin* password is used.

```
aaa authentication enable default group tacacs+ admin
```


aaa authentication iscsi

To configure an iSCSI authentication method list for servers requesting access to storage devices via SCSI routing services, use the `aaa authentication iscsi` command. To delete an iSCSI authentication method list, use the `no` form of this command.

Syntax

```
aaa authentication iscsi default method1 [method2...]
aaa authentication iscsi name method1 [method2...]
no aaa authentication iscsi default
no aaa authentication iscsi name
```

Table 8: Syntax Description

default	Makes the listed authentication methods that follow this argument the default.
name	Makes the listed authentication methods that follow this argument the list of methods used when a user logs in on a scsi router configured with authentication list name
method1 [method2...]	At least one of the methods described in Table 9 .

Defaults

If iSCSI authentication is specified as default and the default authentication list is not configured, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication iscsi default local
```

If iSCSI authentication is specified as *name* and the *name* authentication list is not configured, iSCSI authentication will always fail.

Command Modes

Administrator.

Usage Guidelines

iSCSI authentication uses AAA authentication services for IP hosts and FC server instances that request access to storage devices from SCSI routing instances with authentication enabled.

AAA uses each service in the order listed in the iSCSI default authentication list, until authentication succeeds or fails. If the authentication service fails to find a user name match, authentication fails. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA uses the next service in the list for authentication.

If either the local or local-case authentication service is the first service on the iSCSI authentication list and AAA fails to find a user name match, AAA uses the next method on the list for authentication. If the local or local-case authentication service is in any other position on the list and AAA fails to find a user name match, authentication fails and access is denied. If a RADIUS or TACACS+ server fails to find a user name match (regardless of position on the iSCSI authentication list), authentication fails and access is denied.

Use the `show runningconfig` command to display the current list of authentication services.

Note: In Table 9, the group RADIUS and group TACACS+ methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the `RADIUS-server host` and `TACACS+-server host` commands to configure the host servers.

Table 9: AAA Authentication iSCSI Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
group groupname	Uses the server group groupname.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

Examples

The following example creates a new AAA authentication list. When iSCSI authentication is required, AAA first tries to use the local username database for authentication. If no match is found, AAA attempts to contact a TACACS+ server. If no server is found, TACACS+ returns an error and the user is allowed access with no authentication.

```
aaa authentication iscsi default local group tacacs+ none
```

aaa authentication login

To configure a login authentication method list for users requesting console access to the storage router, use the `aaa authentication iscsi` command. To delete a login authentication method list, use the `no` form of this command.

Syntax

```
aaa authentication login default method1 [method2...]  
no aaa authentication login default
```

Table 10: Syntax Description

default	Makes the listed authentication methods that follow this argument the default.
method1 [method2...]	At least one of the methods described in Table 11 .

Defaults

If the default login authentication list is not configured, only the monitor password is selected. This has the same effect as the following command:

```
aaa authentication login default monitor
```

Command Modes

Administrator.

Usage Guidelines

Login authentication uses AAA authentication services to provide authentication of users requesting console access.

AAA uses each service in the order listed in the login default authentication list, until authentication succeeds or fails. If the authentication service fails to find a user name match, authentication fails. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA uses the next service in the list for authentication.

If either the local or local-case authentication service is the first service on the login authentication list and AAA fails to find a user name match, AAA uses the next method on the list for authentication. If the local or local-case authentication service is in any other position on the list and AAA fails to find a user name match, authentication fails and access is denied. If a RADIUS or TACACS+ server fails to find a user name match (regardless of position on the login authentication list), authentication fails and access is denied.

Use the `show runningconfig` command to display the current list of authentication services.

Note: In [Table 11](#), the group RADIUS and group TACACS+ methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the `RADIUS-server host` and `TACACS+-server host` commands to configure the host servers.

Table 11: AAA Authentication Login Methods

Keyword	Description
<code>enable</code>	Uses the admin password, as specified with the <code>admin password</code> command.
<code>group radius</code>	Uses the list of all RADIUS servers for authentication.
<code>group tacacs+</code>	Uses the list of all TACACS+ servers for authentication.
<code>group groupname</code>	Uses the server group <code>groupname</code> .
<code>local</code>	Uses the local username database for authentication.
<code>local-case</code>	Uses case-sensitive local username authentication.
<code>monitor</code>	Uses the monitor password, as specified with the <code>monitor password</code> command.
<code>none</code>	Uses no authentication.

Examples

The following example creates a new AAA authentication list. When login authentication is required, AAA first contacts a TACACS+ server. If no server is found, the monitor password is used.

```
aaa authentication login default group tacacs+ monitor
```

aaa generate password

To generate a password based on 128 bits of random data, use the `aaa generate password` command.

Syntax

```
aaa generate password
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

To encourage administrators to use passwords that are resistant to an offline dictionary attack, this command is provided to generate hexadecimal string passwords based on 128 bits of random data. When the command is run, a 32-character hexadecimal string is displayed that the administrator can cut and paste to either a `username` command or some host system password utility or file.

Examples

The following command displays a different random password each time it is executed.

```
aaa generate password
```

aaa group server radius

To create a server group that can specify a subset of the RADIUS server hosts defined with the `radius-server host` command, or add a RADIUS server host to a server group, use the `aaa group server radius` command. To delete a RADIUS server group host or the entire group, use the `no` form of this command.

Syntax

```
aaa group server radius name
aaa group server radius name A.B.C.D [auth-port nn]
aaa group server radius name deadtime nn
no aaa group server radius name
no aaa group server radius name A.B.C.D [auth-port nn]
no aaa group server radius name deadtime
```

Table 12: Syntax Description

<code>name</code>	The name of server group to be created, deleted, or modified
<code>A.B.C.D</code>	The IP address of the RADIUS host
<code>auth-port <i>nn</i></code>	The UDP destination port for RADIUS authentication requests. Valid range is 1 to 65535. Default is 1645. (Optional)
<code>deadtime <i>nn</i></code>	The time in minutes that a RADIUS server will be skipped after being determined to be down. Valid range is 1 to 1440 minutes. Default is specified with RADIUS-server <code>deadtime</code> command.

Defaults

By default, only the global RADIUS server list is available.

Command Modes

Administrator.

Usage Guidelines

When a server group is specified as an authentication method, AAA tries each server host, in order, until a valid response is received or a timeout occurs. If the end of the server group is reached, the next authentication method is used.

Examples

The following example creates a server group with two server hosts. The hosts must be created with the `radius-server host` command.

```
aaa group server radius abc
aaa group server radius abc 1.0.0.1
aaa group server radius abc 1.0.0.2
```

aaa group server tacacs+

To create a server group that can specify a subset of the TACACS+ server hosts defined with the `tacacs-server host` command, or add a TACACS+ server host to a server group, use the `aaa group server tacacs+` command. To delete a TACACS+ server group host or the entire group, use the `no` form of this command.

Syntax

```
aaa group server tacacs+ name
aaa group server tacacs+ name A.B.C.D [auth-port nn]
no aaa group server tacacs+ name
no aaa group server tacacs+ name A.B.C.D [auth-port nn]
```

Table 13: Syntax Description

<i>name</i>	The name of server group to be created, deleted, or modified
<i>A.B.C.D</i>	The IP address of the TACACS+ host
auth-port <i>nn</i>	The TCP destination port for TACACS+ authentication requests. Valid range is 1 to 65535. Default is 49. (Optional)

Defaults

By default, only the global TACACS+ server list is available.

Command Modes

Administrator.

Usage Guidelines

When a server group is specified as an authentication method, AAA tries each server host, in order, until a valid response is received or a timeout occurs. If the end of the server group is reached, the next authentication method is used.

Examples

The following example creates a server group with two server hosts. The hosts must be created with the `tacacs-server host` command.

```
aaa group server tacacs+ def
aaa group server tacacs+ def 1.2.0.1
aaa group server tacacs+ def 1.2.0.2
```

aaa new-model

This command exists only for compatibility with IOS and provides no functionality on a storage router. To enable the AAA access control model, issue the `aaa new-model` command. To disable AAA access control model, use the `no` form of this command. There is currently only one model and user cannot be changed. When the command is run, the message “AAA new-model always enabled” is displayed.

Syntax

```
aaa new-model
no aaa new-model
```

This command has no arguments or keywords.

Defaults

AAA is not enabled.

Command Modes

Administrator.

Usage Guidelines

This command enables the AAA access control model. It is available for completeness only; AAA cannot be disabled for the storage router. AAA authentication services provide iSCSI authentication of IP hosts and FC server instances requiring access to storage devices via SCSI routing instances. iSCSI authentication is disabled by default and can be enabled for specific SCSI routing instances using the `scsirouter authenticate` CLI command.

Examples

The following example initializes AAA:

```
aaa new-model
```

aaa test authentication

To test an AAA authentication method for services requesting authentication through AAA, use the `aaa test authentication` command.

Syntax

```
aaa test authentication service list username password
```

Table 14: Syntax Description

<code>service</code>	The authentication service to be tested. Must be either <code>enable</code> , <code>iscsi</code> , or <code>login</code> .
<code>list</code>	The authentication method list to be tested. Must be default if service is <code>enable</code> or <code>login</code> .
<code>username</code>	The user name to be tested.
<code>password</code>	The password associated with the specified user name.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The password displays a series of asterisks (* * * * *) to hide the plain text password being entered.

Examples

The following example tests AAA authentication for the user named user1, with a password of password1:

```
aaa test authentication iscsi default user1 * * * * *
```

aaa test authentication cancel

To cancel any outstanding authentication requests issued with the `aaa test authentication` command, use the `aaa test authentication cancel` command.

Syntax

```
aaa test authentication cancel
```

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

If an entry is made specifying a non-existent RADIUS or TACACS+ server with a long timeout or high retransmit count, an authentication request can be outstanding for a very long time. If enough of these requests become outstanding,

the active request limit will be reached (currently 4), keeping any other requests from being processed. The user must pick some values for timeout and retransmit or use the defaults.

Examples

The following command cancels all outstanding test authentication requests:

```
aaa test authentication cancel
```

debug aaa

To enable debugging for authentication, authorization, and accounting (AAA) services used to provide iSCSI authentication for IP hosts and FC server instances requesting access to storage devices via SCSI routing instances, use the `debug aaa` command. To disable debugging for AAA authentication services, use the `no` form of this command.

Syntax

```
debug aaa  
no debug aaa
```

This command has no arguments or keywords.

Defaults

Debugging is not enabled.

Command Modes

Administrator.

Usage Guidelines

Use this command to debug problems with iSCSI authentication or general AAA authentication services. Change the logging level for the console or the log file to *debugging* to capture the AAA debug message. Debug messages are only written if the logging level is *debugging*.

Examples

The following example enables AAA debugging:

```
debug aaa
```

ip radius source-interface

To specify the interface IP address to use as the source IP address of outgoing RADIUS requests use the `ip radius source-interface` command. To always use the IP address of the outgoing interface use the `no` form of this command.

Syntax

```
ip radius source interface A.B.C.D
no ip radius source interface
```

Table 15: Syntax Description

A.B.C.D	The interface IP address to use as the source IP address of the outgoing RADIUS requests
---------	--

Defaults

Use the IP address of the outgoing interface.

Command Modes

Administrator.

Usage Guidelines

Some RADIUS servers are configured to allow requests from only certain IP addresses. This command can be used to specify which interface IP address to be used for all outgoing RADIUS requests, regardless of which interface they are actually sent from. If this command is not used, or if the interface cannot be found, the IP address of the actual outgoing interface will be used.

Examples

The following command specifies the source IP address of the outgoing RADIUS requests:

```
ip radius source-interface 1.1.1.1
```

ip tacacs source-interface

To specify the interface IP address to use as the source IP address of outgoing TACACS+ requests, use the `ip tacacs source-interface` command. To always use the IP address of the outgoing interface, use the `no` form of this command.

Syntax

```
ip tacacs source interface A.B.C.D
no ip tacacs source interface
```

Table 16: Syntax Description

A.B.C.D	The interface IP address to use as the source IP address of the outgoing TACACS+ requests
---------	---

Defaults

Use the IP address of the outgoing interface.

Command Modes

Administrator.

Usage Guidelines

Some TACACS+ servers are configured to allow requests from only certain IP addresses. This command can be used to specify which interface IP address to be used for all outgoing TACACS+ requests, regardless of which interface they are actually sent from. If this command is not used, or if the interface cannot be found, the IP address of the actual outgoing interface will be used.

Examples

The following command specifies the source IP address of the outgoing TACACS+ requests:

```
ip tacacs source-interface 1.1.1.1
```

radius-server deadtime

To set the global deadtime value for RADIUS servers, use the `radius-server deadtime` command. To delete the global deadtime value, use the `no` form of this command.

Syntax

```
radius-server deadtime nn  
no radius-server deadtime
```

Table 17: Syntax Description

<i>nn</i>	The time in minutes that a RADIUS server will be skipped after being determined to be down
-----------	--

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Depending on the configured retransmit and timeout values, it can take a long time to give up on a RADIUS server host and proceed to the next configured host. To speed future requests, RADIUS server host can be marked as down if no valid response is received after the configured retransmit and timeout values, as specified by the `radius-server deadtime` command. Note that a separate timer is kept for each list the RADIUS server host appears on: one for the global

and one for each server group list. When a host is marked down (by exceeding the retransmit count), it is marked down on all lists, and when a host is marked “up” (by sending a valid response), it is marked up on all lists.

Examples

The following example set the global RADIUS server deadtime to 60 minutes.

```
radius-server deadtime 60
```

radius-server host

To specify a RADIUS server host to be used for AAA authentication for servers requesting access to storage devices via SCSI routing services, use the `radius-server host` command. The `radius-server host` command parameters `auth-port`, `timeout`, `retransmit`, and `key` can be specified in any order. To delete the specified RADIUS server host use the `no` form of this command.

Syntax

```
radius-server host A.B.C.D [[auth-port nn] [timeout nn]
[retransmit nn] [key key]]
no radius-server host A.B.C.D [auth-port nn]
```

Table 18: Syntax Description

A.B.C.D	IP address of the RADIUS server host
auth-port nn	The UDP destination port for RADIUS authentication requests. Valid range is 1 to 65535. Default is 1645 (Optional)

Table 18: Syntax Description (Continued)

<code>key key</code>	Specifies the authentication and encryption key for all RADIUS communications between the storage router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key. This key overrides the global setting of the RADIUS-server key command. If no key string is specified, the global value is used. (Optional)
<code>timeout nn</code>	Specifies the host-specific time interval that the storage router waits for the RADIUS server to reply before retransmitting. Enter a value in the range of 1 to 1000. This setting overrides the global value of the RADIUS-server timeout command. If no timeout value is specified, the global value is used. (Optional)
<code>retransmit nn</code>	Specifies the number of time a RADIUS request is re-sent to this RADIUS server, if this server is not responding or responding slowly. Enter a value in the range of 0 to 100. This setting overrides the global setting of the RADIUS-server retransmit command. If no retransmit value is specified, the global value is used. (Optional)

Defaults

No RADIUS host is specified.

Command Modes

Administrator.

Usage Guidelines

AAA authentication services are used to provide iSCSI authentication for IP hosts and FC server instances requesting access to storage devices.

- You can use multiple `RADIUS-server host` commands to specify multiple RADIUS servers. The software searches for servers in the order in which you specify them.
- If no host-specific timeout, retransmit, or key values are specified, the global values apply to each RADIUS server.
- If you use spaces in the key, enclose the key in quotation marks.

An error message is displayed if `auth-port`, `timeout`, `retransmit`, or `key` parameters are specified more than once.

Always configure the key as the last item in the `RADIUS-server host` command syntax; the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, enclose the key in quotation marks unless the quotation marks themselves are part of the key. The key can not contain both a single and double quote character.

Examples

The following example specifies the host with IP address 172.29.39.46 as the RADIUS server and uses the default port for authentication:

```
radius-server 172.29.39.46
```

The following example specifies port 1612 as the destination port for authentication requests on the RADIUS host 172.29.39.46:

```
radius-server host 172.29.39.46 auth-port 1612
```

The following example specifies the host with IP address 172.29.39.46 as the RADIUS server, uses ports 1612 as the authorization port, sets the timeout value to 6, sets the retransmit value to 5, and sets "rad123" as the encryption key, matching the key on the RADIUS server:

```
radius-server host 172.29.39.46 auth-port 1612 timeout 6 retransmit  
5 key rad123
```

radius-server key

To set the authentication and encryption key to be used for all RADIUS communications between the SR 2122 Storage Router and the RADIUS daemon, use the `radius-server key` command. To delete the key, use the `no` form of this command.

Syntax

```
radius-server key key-string
no radius-server key
```

Table 19: Syntax Description

key-string	The authentication and encryption key string to be used for all RADIUS communications, in clear text. If spaces are used in the key, enclose the key in quotation marks.
------------	--

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

After configuring authentication services for iSCSI authentication with the `aaa authentication iscsi` command, use the `radius-server key` command to set the global authentication and encryption key. The key entered as part of the command must match the key used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key enclose the key in quotation marks unless the quotation marks themselves are part of the key (i.e. “my key string”).

To override the global key for a specific RADIUS server, use the `radius-server host` command with the **key** keyword.

Examples

The following example sets the global authentication and encryption key to “my key string”.

```
radius-server key "my key string"
```

radius-server retransmit

To specify the number of times the SR 2122 Storage Router resends the RADIUS request to the each server in the list of configured RADIUS servers after a timeout occurs, use the `radius-server retransmit` command. To restore the default use the `no` form of this command.

Syntax

```
radius-server retransmit nn  
no radius-server retransmit
```

Table 20: Syntax Description

nn	The number of times the request can be resent to each server in the list. Valid range is 0 to 100. The default is 3 .
----	--

Defaults

The number of possible resends default is three.

Command Modes

Administrator.

Usage Guidelines

If multiple RADIUS servers are configured for AAA authentication, the storage router attempts to reach each server in the list before incrementing the retransmit count.

To override the global retransmit count for a specific RADIUS server, use the `radius-server host` command with the **retransmit** keyword.

Examples

The following example sets the retransmit count to six, meaning the request can be resent up to six time for every RADIUS server:

```
radius-server retransmit 6
```

radius-server timeout

To set the global interval that the SR 2122 Storage Router waits for a RADIUS server host to reply, use the `radius-server timeout` command. To restore the default, use the `no` form of this command.

Syntax

```
radius-server timeout nn  
no radius-server timeout
```

Table 21: Syntax Description

<i>nn</i>	Specifies the global timeout value in seconds. Valid range is 1 to 1000. The default is 5.
-----------	--

Defaults

The timeout value defaults to five seconds.

Command Modes

Administrator.

Usage Guidelines

Use this command to set the number of seconds the storage router waits for a RADIUS server host to reply before timing out.

To override the global timeout value for a specific RADIUS server, use the `radius-server host` command with the **timeout** keyword.

Examples

The following example sets the global timeout value to 10. You can increase the timeout value if you have network problems or if the RADIUS servers are slow to response, causing consistent timeouts when a lower timeout value is used.

```
radius-server timeout 10
```

scsirouter authentication

To enable iSCSI authentication using AAA authentication services for the named SCSI routing instance, use the `scsirouter authenticate` command.

Syntax

```
scsirouter name authentication none
scsirouter name authentication default
scsirouter name authentication list
```

Table 22: Syntax Description

name (?)	The name of this SCSI routing instance
none	No iSCSI authentication is done
default	iSCSI authentication is done using the default iSCSI authentication method list.
list	iSCSI authentication is done using the iSCSI authentication method list name.

Defaults

iSCSI authentication is disabled.

Command Modes

Administrator.

Usage Guidelines

Use the `scsirouter authentication` command to enable iSCSI authentication for IP hosts requesting access to storage devices using the named SCSI routing instance. AAA performs authentication using the services configured on the iSCSI authentication method list. Use the `aaa authentication iscsi` command to configure the iSCSI authentication method list.

If authentication is specified as **default** for a SCSI routing instance, but no default iSCSI authentication method list has been defined, AAA uses the local username database.

Examples

The following example enables AAA authentication for the SCSI routing instance named *fool*:

```
scsirouter fool authentication default
```

show aaa

To display authentication, authorization, and accounting (AAA) configuration information and operational statistics, use the `show aaa` command.

Syntax

```
show aaa [stats]
show aaa [from {filename | bootconfig | runningconfig}]
```

Table 23: Syntax Description

<code>stats</code>	Displays the number of authentication requests received and sent since the storage router was last rebooted (Optional)
from <i>filename</i>	The name of the configuration file where the AAA configuration is stored. This file must exist in the <i>savedconfig</i> directory. (Optional)
<code>from bootconfig</code>	Display the AAA information from the persistent saved configuration. (Optional)
<code>from runningconfig</code>	Display the AAA information from the currently running configuration. (Optional)

Defaults

If no **from** parameter is specified, the display shows information from the currently running configuration.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to determine the current AAA configuration for the storage router. Use the **stats** keyword to display usage statistics. Use the **from bootconfig** keywords to display the specified AAA configuration information as it exists in the current saved configuration, used when the storage router restarts. This may differ from the running configuration. If no requests are outstanding then received should equal "sent + canceled" and sent should equal "passed + failed."

Table 24: show aaa command fields

Field Name	Data Format	Description
Requests received	decimal	Number of authentication requests received
Responses sent	decimal	Number of authentication requests sent
Requests Canceled	decimal	Number of auth requests that were canceled either by the aaa test authentication cancel command or by the SCSI TCP server or client
Requests Passed	decimal	Number of auth requests that passed authentication
Requests Failed	decimal	Number of auth requests that failed authentication

Examples

The following example output displays the current AAA authentication configuration for the storage router. The authentication list indicates that authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the local username database for

authentication. If a match is found, the user is allowed access; if no match is found, the user is denied access. If this attempt also returns an error, the user is allowed access with no authentication.

```
show aaa
aaa new-model
aaa authentication iscsi default group radius group tacacs+ local
username "bob" password "9 72c169b9b1c3510de3bc9d014c5e706484"
radius-server host 161.44.68.80 auth-port 1812 key "9
3c99ecd17d937eff1e2a2f52b9635190c0"
tacacs-server key "9
3b721b69d67a9b390f46e3711f2abe3f879e10b2375a5604ba3a5a10f703937928
"
tacacs-server host 161.44.68.80 auth-port 49 key "9
9272e435f03b00bc84e09019596b9da7b2"
```

The following is example output from the show aaa stats command:

```
show aaa stats
authentication requests received = 2
authentication responses sent = 2
authentication requests canceled = 0
authentication requests passed = 2
authentication requests failed = 0
```

RADIUS Server Hosts				
IP Address	port	timeouts	bad	resps
-----	----	-----	---	-----
161.44.68.80	1812	2		7

TACACS+ Server Hosts				
IP Address	port	timeouts	bad	resps
-----	----	-----	---	-----
161.44.68.80	49	0		2

The following is example output for the show aaa from bootconfig command:

```
show aaa from bootconfig
aaa new-model
aaa authentication iscsi default group tacacs+ local
username "fred" password "9 af4f2428498a41a31e237de1c4a9b9fcef"
username "pat" password "9 7ddbccc3d0daf013f4293c3d3bd94539dd"
username "kris" password "9 0607167520058771e66ab1d379d7e6505f"
username "adrian" password "9 0ad24a3b35dc296d894e512416d572b3ee"
radius-server retransmit 12
radius-server host 10.5.0.53 auth-port 1645
tacacs-server timeout 12
tacacs-server host 10.7.0.22 auth-port 49
```

tacacs-server host

To specify a TACACS+ server to be used for AAA authentication services, use the `tacacs-server host` command. To delete the specified TACACS+ server host use the `no` form of this command.

Syntax

```
tacacs-server host A.B.C.D [auth-port nn] [timeout nn] [key key]
no tacacs-server host A.B.C.D [auth-port nn]
```

Table 25: Syntax Description

A.B.C.D	The IP address of the TACACS+ host.
auth-port <i>nn</i>	The TCP destination port for TACACS+ authentication requests. Valid range is 1 to 65535. Default is 49. (Optional)
timeout <i>nn</i>	The amount of time in seconds the storage router should wait for a reply from a TACACS+ server before timing out. Valid range is 1 to 1000. This setting overrides the global setting of the <code>tacacs-server timeout</code> command. If no timeout value is specified, the global value is used. (Optional)
key <i>key</i>	Specify the authentication and encryption key for all TACACS+ communication between the storage router and this TACACS+ host. The character string must match the key used by the TACACS+ daemon. This key overrides the global setting of the <code>tacacs-server key</code> command. If no key string is specified, the global value is used. If spaces are part of the key string, enclose the string in quotation marks. (Optional)

Defaults

No TACACS+ host is specified.

Command Modes

Administrator.

Usage Guidelines

AAA authentication services provide iSCSI authentication for IP hosts and FC server instances requesting access to storage resources.

- You can use multiple `tacacs-server host` commands to specify additional hosts. The storage router searches for hosts in the order in which you specify them.
- If no host-specific timeout or key values are specified, the global values apply to each host.
- Always configure the key as the last item in the `tacacs-server host` command syntax. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key enclose the key in quotation marks unless the quotation marks themselves are part of the key. Note the key cannot contain both a single and double quote character.

Because some of the parameters of the `tacacs-server host` command override global settings made by the `tacacs-server timeout` and `tacacs-server key` commands, you can use this command to enhance security on your network by uniquely configuring individual storage routers.

Examples

The following example specifies the server with IP address 172.29.39.46 as the TACACS+ server and uses the default port for authentication:

```
tacacs-server 172.29.39.46
```

The following example specifies port 52 as the destination port for authentication requests on the TACACS+ host 172.29.39.46:

```
tacacs-server host 172.29.39.46 auth-port 52
```

The following example specifies the host with IP address 172.29.39.46 as the TACACS server, uses ports 52 as the authorization port, sets the timeout value to 6, and sets `tac123` as the encryption key, matching the key on the TACACS+ server:

```
tacacs-server host 172.29.39.46 auth-port 52 timeout 6 key tac123
```

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the storage router and the TACACS+ daemon, use the `tacacs-server key` command. To delete the key use the `no` form of this command.

Syntax

```
tacacs-server key key  
no tacacs-server key
```

Table 26: Syntax Description

key	The authentication and encryption key string to be used for all TACACS+ communications, in clear text. If spaces are part of the key string, enclose the string in quotation marks.
-----	---

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

After using the `aaa authentication iscsi` command to configure the iSCSI default authentication list to use TACACS+ authentication services, use the `tacacs-server key` command to set the global authentication and encryption key. The key entered as part of the command must match the key on the TACACS+ daemon. If spaces are part of the key string, enclose the key string in quotation marks.

To override the global key for a specific TACACS+ server, use the `tacacs-server host` command with the **key** keyword.

Examples

The following example sets the global authentication and encryption key to “my TACACS key string”:

```
radius-server key "my TACACS key string"
```

tacacs-server timeout

To set the global interval that the SR 2122 Storage Router waits for a TACACS+ host to reply, use the `tacacs-server timeout` command. To restore the default, use the `no` form of this command.

Syntax

```
tacacs-server timeout nn
no tacacs-server timeout
```

Table 27: Syntax Description

<i>nn</i>	Specifies the global timeout value, in seconds. Valid range is 1 to 1000. The default is 5.
-----------	---

Defaults

The timeout value defaults to five seconds.

Command Modes

Administrator.

Usage Guidelines

Use this command to set the number of seconds the storage router waits for a TACACS+ host to reply before timing out.

To override the global timeout value for a specific TACACS+ host, use the `tacacs-server host` command with the **timeout** keyword.

Examples

The following example sets the global timeout value to 10. You can increase the timeout value if you have network problems or if TACACS+ hosts are slow to response, causing consistent timeouts when a lower timeout value is used.

```
tacacs-server timeout 10
```

username password

To build a local username database to be used with the local method of AAA authentication services, use the `username password` command. To delete the specified user name, use the `no` form of this command.

Syntax

```
username username password password
username username password "0 password"
username username password "9 password"
no username username
```

Table 28: Syntax Description

<code>username</code>	A valid user name
<code>username</code> (?)	Enter an existing user name
<code>password</code>	Unencrypted password associated with the specified user name
<code>0 password</code>	Unencrypted password associated with the specified user name. Allows user to specify a password that starts with a 0 (0 0xxx) or 9 (0 9xxx).
<code>9 password</code>	Encrypted password using SRBU private encoding. Password is associated with the specified user name.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `username password` command to build the local username database. Use the `aaa authentication iscsi` command to configure the iSCSI default authentication list to use local or local-case authentication services. The AAA authentication service local-case performs a case-sensitive user name match; the local service user name match is not case-sensitive. Both local and local-case use case-sensitive password matching for authentication.

To display the contents of the local username database, issue the `show aaa` command.

Examples

The following example configures two user names (*foo1* and *foo2*) and password (*foo1password* and *encrypted password*):

```
username foo1 password foo1password
username foo2 password "9 1234abcd1234abcd1234abcd1234abcd12"
To display the user name database, issue the show aaa command. The
following is example output from the show aaa command:
show aaa
aaa new-model
aaa authentication iscsi default group tacacs+ local none
username foo1 password <password>
username foo2 password "9 1234abcd1234abcd1234abcd1234abcd12"
```

username password

Administrative Commands

3

This section describes all CLI commands related to the administration of the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

admin contactinfo

To provide basic contact information for the administrator of this HP SR2122-2 Storage Router, use the `admin contactinfo` command.

Syntax

```
admin contactinfo name text
admin contactinfo email text
admin contactinfo phone text
admin contactinfo pager text
admin contact info name text email text phone text pager text
```

Table 29: Syntax Description

<code>name <i>text</i></code>	The name of the storage router administrator (Optional)
<code>email <i>text</i></code>	The e-mail address of the storage router administrator. This is an address to which alerts may be sent. (Optional)
<code>phone <i>text</i></code>	The phone number of the storage router administrator (Optional)
<code>pager <i>text</i></code>	An optional pager number (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `admin contactinfo` command to provide site-specific information associated with the storage router. The command accepts each parameter separately, or all parameters together. If all parameters are specified, they must be in the sequence shown. Usage is completely site-specific.

Enclose each string containing spaces in single or double quotes. If a string contains a single quote, enclose it in double quotes; if it contains a double quote, enclose it in single quotes. A string cannot contain both single and double quotes, this avoids having to use escape characters.

Examples

The following commands set the system administrator name and e-mail address:

```
admin contactinfo name "Pat Hurley"  
admin contactinfo email "hurley@abc123z.com"
```

The following command sets all system administrator contact information:

```
admin contactinfo name "Chris Smith" email  
"chris.smith@zxy478x.com" phone "123.555.5555 ext 97" pager  
"123.456.3444 pin 2234"
```

admin password

To set the password used for administrative access to the SR 2122 Storage Router management interface, use the `admin password` command. Access may be via Telnet (for CLI), or web-based graphical user interface (GUI).

Syntax

```
admin password password
```

Table 30: Syntax Description

password	The password associated with administrative access to the storage router management interface. The string can be enclosed in quotes, and must be enclosed in quotes if the password includes one or more spaces. Enclose the string in quotes. A string value of "" clears the password. The default password is hp.
----------	--

Defaults

The default password is **hp**.

Command Modes

Administrator.

Usage Guidelines

The storage router's management interface is password protected. You must enter passwords when accessing the storage router via Telnet (for CLI) or web-based GUI. The Monitor-mode password provides view-only access to management interface, while the Administrator mode password allows the user to create entities and make changes to the configuration of the storage router. Password protection can also be extended to the storage router console, using the `restrict console` command.

The password can contain one or more spaces, if the password string is enclosed in quotes. A string value of "" clears the password, effectively setting it to nothing.

Note: The password is displayed in clear text as the command is entered, but it is changed to a series of pound signs (#####) when the change is acknowledged.

Examples

The following example sets the Administrator mode password to *foo73G*. All passwords are case-sensitive.

```
admin password foo73G
```

delete script

To remove all files or a named file from the `script` directory, use the `delete script` command.

Syntax

```
delete script all
delete script command_file
```

Table 31: Syntax Description

<code>command_file (?)</code>	The name of the command file to be deleted. This file must exist in the script directory.
<code>all</code>	Keyword, indicating that all command files in the script directory will be deleted

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `show script` command to display the contents of the `script` directory or the specified command file.

Examples

The following example removes the command file named `foo_config` from the script directory.

```
delete script foo_config
```

enable

To change the management session from Monitor to Administrator mode, use the `enable` command. Monitor mode, which is the default mode, provides view-only access to the storage router's management interface. Administrator mode allows the user to create entities and make changes to the configuration of the storage router.

Syntax

```
enable
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Monitor.

Usage Guidelines

Issue the `enable` command after a successful CLI login to change to Administrator mode. You are prompted to enter the Administrator-mode password, if required. To return from the Administrative mode to the Monitor mode use the `exit` command.

Examples

The following example changes the mode to administration:

```
enable
Enter admin password: *****
[Entering Administrative mode]
```

exit

To return the management session to Monitor mode from Administrator mode, use the `exit` command.

Syntax

`exit`

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `exit` command to return to Monitor mode after issuing the `enable` command.

Examples

The following example returns the CLI session to Monitor mode:

```
exit
[Leaving Administrative mode]
```

halt

To prepare the storage router to be powered down, issue the `halt` command.

Syntax

```
halt [force] [fast]
```

Table 32: Syntax Description

<code>fast</code>	Bypass hardware diagnostics when the storage router is next restarted (Optional)
<code>force</code>	Force an immediate halt of the storage router (Optional)

Defaults

If there are unsaved configuration changes when the command is issued, the default is to save all changes before halting. If the command is issued with the optional **force** keyword, any unsaved configuration changes are discarded.

Command Modes

Administrator or Monitor.

Usage Guidelines

The `halt` command prepares the storage router file system to be powered down. If the storage router is participating in a cluster, the `halt` command causes any SCSI routing instances running on this storage router to fail-over to another storage router in the cluster. If the `halt` command is issued with no keywords and there are unsaved changes to the current configuration, you are prompted to save or discard the changes. Use the **force** keyword to cause an immediate halt of the storage router, discarding any unsaved configuration changes. Append the optional **fast** keyword to bypass diagnostics when the storage router is restarted. When the `halt` command completes, the storage router displays the following system prompt:

```
halt
[HALTED] #
```


The storage router can be safely powered down when the HALTED system prompt appears. The only CLI command that can be issued from the storage router at the HALTED system prompt is the `reboot` command.

When the storage router is restarted, the cluster determines any SCSI routing instances that should start on the storage router. If the storage router is identified as the preferred storage router for any SCSI routing instance (via the `scsirouter primary` command), that instance will start running on the storage router.

Examples

Use the following `halt` command (without the **force** keywords) and if there are unsaved changes to the current configuration, you are prompted to save or discard the changes:

```
halt
```

help

To display information about how to use the CLI, issue the `help` command.

Syntax

```
help
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

The `help` command displays information about the various CLI commands that can be issued, based on the mode currently in use. The `help` command also displays information about the special keys that can be used in the CLI.

Examples

The following example displays the basic monitor commands and a description of the special keys resulting from the `help` command:

```
help
```

hostname

To set the system name for the storage router, use the `hostname` command. The storage router is recognized by this name through the management interface. This command takes effect immediately and the new system name is automatically integrated into the prompt string.

Syntax

```
hostname sysname
```

Table 33: Syntax Description

<i>sysname</i>	The name of the storage router. This may be the fully-qualified domain name. Maximum length is 19 characters. The name cannot contain blanks, white space, or control characters.
----------------	---

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

All storage routers must have a system name. To enable network management on the storage router using the facilities of a Domain Name Server (DNS), you must make the storage router's system name and IP address known to that DNS. Use the system name specified in this command.

Examples

In the following command, the storage router name is set to *sr2122_lab1*.

```
hostname SR2122_lab1
```

logout

To terminate the current CLI management session, use the `logout` command.

Syntax

```
logout
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Depending on the mode and whether you are connected via the serial port or remotely via telnet, `logout` acts differently:

- If a user is connected to the storage router in Administrator mode or Monitor mode via a Telnet sessions, the `logout` command terminates the CLI management session. No CLI commands can be issued until you log in again.
- If a user is connected to the storage router in Administrative mode via the console interface, the `logout` command returns the session to Monitor mode (like the `exit` command).
- If a user is connected to the storage router in Monitor mode via the console interfaces, the `logout` command has no effect.

Examples

None.

monitor password

To set the password used for view-only access to the SR 2122 management interface, use the `monitor password` command. Access may be via Telnet (for CLI), or web-based graphical user interface (GUI).

Syntax

```
monitor password password
```

Table 34: Syntax Description

<code>password</code>	The case-sensitive password associated with view-only access to the storage router's management interface. The default password is <code>hp</code> .
-----------------------	--

Defaults

The default password is **hp**.

Command Modes

Administrator.

Usage Guidelines

The storage router’s management interface is password protected. You must enter passwords when accessing the storage router via the CLI or web-based GUI. Passwords can be also applied to the console interface. The Monitor-mode password provides view-only access to storage router’s management interface, while the Administrator-mode password allows the user to create entities and make changes to the configuration of the SR 2122 system.

Set the password string to “ ” clears the password, effectively setting it to nothing.

Note: The password is displayed in clear text as the command is entered, but it is changed to a series of pound signs (#####) when the change is acknowledged.

Examples

The following example sets the Monitor-mode password to *M17g23*. All passwords are case-sensitive.

```
monitor password M17g23
```

read

To execute CLI commands contained within a command file, use the `read` command.

Syntax

```
read script command_file [force]
```

Table 35: Syntax Description

<code>command_file</code> (?)	The name of the command file. Use the “?” to get the list of existing command files.
<code>force</code>	Suppresses warning prompts and messages (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

If you have a set of CLI commands that you run periodically, you can place them in a command file and use the `read` command to execute them when needed. When the command is issued without the **force** keyword, you are prompted to confirm your actions and reminded that the actions may change the configuration of the storage router.

You can also use the command file created from executing a `show {runningconfig | bootconfig} filename` command. This scenario is used as a basis to clone an initial configuration on another SR 2122.

The `read` command assumes you copied the command file into the `/ata0/script` directory. The `read` command assumes the file is ascii text. The user can get the list of `read` command files by executing the following command `read script ?` which returns the list of files contained in the `/ata0/script` directory. To delete a `read` command file, the command `delete script <command_file>` is used. To get the list of files which can be deleted execute the `delete script ?` command.

The command `read <command_file>` reads the commands from the specified command file one line at a time. The command is executed only if the parser finds it syntactically correct and no errors are detected by error checking the arguments. The parser echoes each command before the command is executed. If the command is executed but returns an exit status not equal to OK, the error message "Executing command %s from file %s returned error code %d" is displayed.

Example:

```
logging buffered level debugging
logging console level debugging
```

You can add a comment by putting the `!` or `#` character at position zero or the first character of the line. This is useful to document what is being done. It can also be used to comment out command arguments or entire commands that may not be used currently but should not be removed from the file.

Example:

```
# Displaylog file size
show logging size
```

Example:

```
logging buffered level \  
! debugging  
! errors  
warnings
```

Continuation character

If a continuation character ‘\’ is added to the end of a line, a command can be extended across line boundaries. The line continuation goes until a line without a continuation character is found and the line is not commented out. End the continuation sequence by adding a blank line after the sequence.

Example:

```
failover scsirouter \  
bob \  
to server1
```

Example: comment ends line continuation

```
failover scsirouter bob to  
server2 \  
# server1 \  
<required a blank line here to end line continuation sequence>  
show interface brief
```

Examples

The following example reads and executes the CLI commands in the command file named *myCommands*.

```
read myCommands
```

myCommands file contains the following commands:

```
logging buffered level debug  
debug scsirouter bob scsitrace
```

reboot

To shut down and then restart the storage router issue the `reboot` command.

Note: Rebooting may cause the SR 2122 to run a different version of software. See the `software version` command for details.

Syntax

```
reboot [force] [fast]
```

Table 36: Syntax Description

<code>fast</code>	Keyword forcing a soft reboot of the storage router, bypassing hardware diagnostics (Optional)
<code>force</code>	Keyword forcing immediate reboot of the storage router (Optional)

Defaults

If there are unsaved configuration changes when the command is issued, the default is to save all changes before rebooting. If the command is issued with the optional **force** keyword, any unsaved configuration changes are discarded.

Command Modes

Administrator.

Usage Guidelines

If the storage router is participating in a cluster, the `reboot` command will cause any SCSI routing instances running on this storage router to fail over to another storage router in the cluster. At restart, the cluster determines any instances of SCSI routing services that should start on the storage router. If the storage router is identified as the preferred SR 2122 for any SCSI routing instance (via the `scsirouter primary` command), that instance starts running on the storage router.

If the `reboot` command is issued with no keywords and there are unsaved changes to the current configuration, you are prompted to either save all changes, to save specific areas that have been modified, or to reboot without saving any changes.

Use the **force** keyword to cause an immediate reboot of the storage router, discarding any unsaved configuration changes. Append the optional **fast** keyword to bypass diagnostics during the reboot sequence.

Examples

The following prompt is received if you issue a `reboot` command (without the **force** keywords) when the storage router has unsaved configuration changes.

```
reboot
Changes have been made to the current configuration of the system
which have not been saved.
yes - all of the configuration data will be saved
no - modifications to the configuration data will not be saved.
prompt - you will be prompted to save the areas that have been
modified.
```

```
Save ALL configuration data? [yes/no/prompt/CTRL-C to abort (yes)]
```

show admin

To display the system administrator contact information, use the `show admin` command.

Syntax

```
show admin
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

The following information displays:

- Contact name
- E-mail
- Phone
- Pager

Examples

The following example displays the system administrator contact information:

```
show admin
Administrator Contact Information
Name: Pat Hurley
Email: phurley@abc123z.com
Phone: 123.456.7890
Pager: 123.456.3444 pin 2234
```

show buffers

To display buffer pool information for a variety of areas, use the `show buffers` command.

Syntax

```
show buffers
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

The display includes the number of free memory buffers for each pool, along with those currently allocated to various functions. The `show buffers` command is designed for debug purposes, and should be used under the guidance of an HP Technical Support professional.

Examples

The following shows sample output from the `show buffers` command:

```
show buffers
```

```
Pool System:
```

```
type      number
```

```
-----
```

```
FREE : 40331
```

```
DATA : 0
```

```
HEADER : 0
```

```
SOCKET : 6
```

```
PCB : 10
```

```
RTABLE : 25
```

```
HTABLE : 0
```

```
ATABLE : 0
```

```
SONAME : 0
```

```
ZOMBIE : 0
```

```
SOOPTS : 0
```

```
FTABLE : 0
```

```
RIGHTS : 0
```

```
IFADDR : 9
```

```
CONTROL : 0
```

```
OOBDATA : 0
```

```
IPMOPTS : 0
```

```
IPMADDR : 3
```

```
IFMADDR : 0
```

```
MRTABLE : 0
```

```
TOTAL : 40384
```

```
number of mbufs: 40384
```

```
number of times failed to find space: 0
```

```
number of times waited for space: 0
```

```
number of times drained protocols for space: 0
```

```
-----  
CLUSTER POOL TABLE
```

```
-----  
size    clusters free    usage
```

```
-----
```

```
64      44      27      23
```

```
128     16499   16481   44
```

```
256     56      44      14
```

```
512     59      53      30
```

```
-----
```

Pool Data:

type number

FREE : 4500

DATA : 0

HEADER : 0

SOCKET : 0

PCB : 0

RTABLE : 0

HTABLE : 0

ATABLE : 0

SONAME : 0

ZOMBIE : 0

SOOPTS : 0

FTABLE : 0

RIGHTS : 0

IFADDR : 0

CONTROL : 0

OOBDATA : 0

IPMOPTS : 0

IPMADDR : 0

IFMADDR : 0

MRTABLE : 0

TOTAL : 4500

number of mbufs: 4500

number of times failed to find space: 0

number of times waited for space: 0

number of times drained protocols for space: 0

CLUSTER POOL TABLE

size clusters free usage

64 4249 4249 6

128 81 81 2083

256 35 35 167

512 36 36 16

1024 23 23 0

2048 23 23 40016

Pool GbE:

type	number
-----	-----

FREE : 16404

DATA : 0

HEADER : 0

SOCKET : 0

PCB : 0

RTABLE : 0

HTABLE : 0

ATABLE : 0

SONAME : 0

ZOMBIE : 0

SOOPTS : 0

FTABLE : 0

RIGHTS : 0

IFADDR : 0

CONTROL : 0

OOBDATA : 0

IPMOPTS : 0

IPMADDR : 0

IFMADDR : 0

MRTABLE : 0

TOTAL : 16404

number of mbufs: 16404

number of times failed to find space: 0

number of times waited for space: 0

number of times drained protocols for space: 0

CLUSTER POOL TABLE

size	clusters	free	usage
-----	-----	-----	-----

Pool FC:

type	number
-----	-----

FREE : 276

DATA : 0

HEADER : 0

```
SOCKET : 0
PCB : 0
RTABLE : 0
HTABLE : 0
ATABLE : 0
SONAME : 0
ZOMBIE : 0
SOOPTS : 0
FTABLE : 0
RIGHTS : 0
IFADDR : 0
CONTROL : 0
OOBDATA : 0
IPMOPTS : 0
IPMADDR : 0
IFMADDR : 0
MRTABLE : 0
TOTAL : 276
number of mbufs: 276
number of times failed to find space: 0
number of times waited for space: 0
number of times drained protocols for space: 0
```

CLUSTER POOL TABLE

size	clusters	free	usage
------	----------	------	-------

Pool iSCSI:

Net Buffers:

type	number
FREE	638
USED	2
TOTAL	640

show cli

To display information about the storage router CLI, use the `show cli` command.

Syntax

```
show cli [commands]
```

Table 37: Syntax Description

commands	Displays one or more specified commands instead of the entire CLI command tree. Note commands are always displayed in alphabetical order. (Optional)
----------	--

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show cli` command to display the complete CLI command tree, along with helpful information about command parameters and arguments. Use the *command-keyword* argument to display information about a specific set of commands, such as `scsirouter` commands. Only valid commands for the current command mode will be displayed.



WARNING: The `show cli` commands with no arguments print large amounts of output since it shows the entire CLI command tree.

Examples

The following shows example output from the `show cli` command, showing the CLI command tree information for the `ping` command:

```
show cli ping
ping          Send ICMP pings to a host
<A.B.C.D>     IP address or hostname to ping
numpkts       Number of packets to attempt
<npkts>       Integer (Default is 5)
size          Size of packet
<sn>          Integer (Default is 64)
size          Size of packet
<sn>          Integer (Default is 64)
```

show cpu

To display CPU utilization information, use the `show cpu` command.

Syntax

```
show cpu
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to view the percentage of CPU utilization for the last five seconds, the last minute, and the last five minutes. The `show cpu` command is designed for debugging purposes; it should be used under the guidance of an HP Technical Support professional.

Examples

The following is example output from the `show cpu` command:

```
show cpu
CPU Utilization for last 5 seconds:1%; last 1 minute:0%; last 5
minutes:0%
```

show crash

To display saved crash trace information from the last crash detected by the system or current crash trace information for debug purposes, use the `show crash` command.

Syntax

```
show crash [current]
```

Table 38: Syntax Description

current	Generates and displays the current crash trace information. This information is the same information that would be generated and saved if the device had crashed. (Optional)
---------	--

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

The default crash trace file is *crash.txt* in the `log` directory. This file is created if the storage router unexpectedly restarts. Use the **current** keyword to display the crash trace information for the storage router. To save the `show crash` command output, redirect the output of your console using the logging facilities for your specific console interface. Depending on your console interface and scroll buffer size, you may also be able to copy and paste the contents from your console into an ASCII text file.

The `show crash` command is designed for debugging purposes; it should only be used under the guidance of an HP Technical Support professional.

Examples

In the following example, no saved crash trace information exists. This condition occurs when the command is issued and the storage router has never unexpectedly restarted.

```
show crash
No crash information available
```

show diagnostics

To show that the hardware passed diagnostic tests on startup, use the `show diagnostics` command.

Syntax

```
show diagnostics
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

The `show diagnostics` command is designed for debugging purposes; it should be used under the guidance of an HP Technical Support professional.

Examples

The following is example output from the `show diagnostics` command:

```
show diagnostics
SR 2122 Hardware Diagnostics Passed.
```

show memory

To display information about memory and related resources in the storage router, use the `show memory` command.

Syntax

```
show memory
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display information about the storage router memory usage. The `show memory` command is designed for debugging purposes; it should be used under the guidance of an HP Technical Support professional.

Examples

The following displays example output from the `show memory` command:

```
show memory
Memory:120079904      Available:44642264
Free Blocks:73        Max Free Block Size:39112096
File Descriptors:256  Available:174
```

Buffer Memory:

Buffer Pool	Total Blocks	Free Blocks	Total Mbufs	Free Mbufs	Warnings
System	16658	16593	40384	40319	
Data	4447	4443	4500	4496	
GbE(1)	16384	16131	16404	16404	
FC(1)	256	256	276	276	
iSCSI	0	0	1024	1024	

show modules

To display addressing information for the modules included in the storage router, use the `show modules` command.

Syntax

```
show modules
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display the memory locations for each module of the storage router software. The `show modules` command is designed for debugging purposes; it should be used under the guidance of an HP Technical Support professional.

Table 39: Show Modules Output

Name	Description
module name	Name of the SR 2122 module
module id	ID
group number	Group number
text start	Start address of the text area
data start	Start address of the data area
bss start	Start address of heap space

Examples

The following shows example output from the `show modules` command:

```
Modules
MODULE NAME      MODULE ID      GROUP #      TEXT START      DATA START
  BSS START
-----
sysInit.out      0x657f48       2            0x64fe70        0x656b30
  0x656bd8
crashDump.out    0x75ded60      3            0x6b7d200       0x6b82130
  0x6b82180
```

show restrict

To display current restrictions on the use of the HP SR2122-2 Storage Router console, interfaces and ports, use the `show restrict` command.

Syntax

```
show restrict
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to identify the current SR 2122 access restrictions.

Examples

The following shows example output from the `show restrict` command. The output shows that passwords are not enabled for the storage router console. All interfaces are closed to FTP. The HA interface and Gigabit Ethernet interfaces are also closed to Telnet. The Gigabit Ethernet interfaces are closed to HTTP. All interfaces are open to SNMP.

```
show restrict
Interface Port   Status Protocol
-----
mgmt      21    closed ftp
          23    open  telnet
          80    open  http (static)
          161   open  snmp

ha        21    closed ftp
          23    closed telnet
          80    open  http (static)
          161   open  snmp

ge1       21    closed ftp
          23    closed telnet
          0     closed http
          161   open  snmp

ge2       21    closed ftp
          23    closed telnet
          80    closed http
          161   open  snmp
```

Console Passwords: enabled

show script

To list all routes available files in the `script` directory or to view the contents of a specific command file, use the `show script` command. Configuration files are stored in the `script` directory.

Syntax

```
show script [ filename ]
```

Table 40: Syntax Description

filename	The name of the configuration file to display. This file must exist in the savedconfig directory. (Optional)
----------	--

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display a list of files in the `script` directory before attempting to execute the commands in the script using the `read` command. Use the *filename* parameter to view the contents of the specified command file.

Examples

The following shows example output from the `show script` command:

```
show script
myscript
testscript
```

show sessions

To display information about active Telnet or GUI sessions to the storage router, use the `show sessions` command.

Syntax

```
show sessions {all | cli | gui}
```

Table 41: Syntax Description

all	Displays all active storage router Telnet or GUI management sessions
cli	Displays only active Telnet (CLI) sessions
gui	Displays only active GUI sessions

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

There are a maximum of 16 concurrent CLI management sessions per storage router. The sessions are restricted as follows:

- One session is reserved for the EIA/TIA-232 console interface.
- There can be a maximum of seven CLI sessions via Telnet or SSH.
- There can be a maximum of eight GUI sessions via HTTP or HTTPS.

Examples

The following shows example outputs from the `show sessions` command. The asterisk designates the CLI management session from which the command was issued.

```
show sessions cli
* 1 console from console as Monitor 1 of 16 sessions
show sessions gui
  1 10.1.30.60 from 10.1.0.2 as Monitor
  2 10.1.30.60 from 10.1.0.2 as Monitor
  2 of 16 sessions
show sessions all
*1 console from console as Administrator (p=0 s=27)
  2 10.1.30.60 from 10.1.0.2 as Monitor (p=36891 s=28)
  3 0.1.30.60 from 10.1.0.2 as Monitor (p=36892 s=32)
  3 of 16 sessions
show sessions all
```

	Id	Auth	From	Login	
	----	-----	-----	-----	
*	1	monitor	console	Mar 22 17:19:10	[TELNET]
	2	admin	10.1.40.212	Mar 22 11:44:46	[TELNET]
	3	admin	10.3.12.222	Mar 22 11:47:12	[GUI]

```
3 of 16 sessions
```

show stack

To display usage of the stack on a per-task basis, use the `show stack` command.

Syntax

```
show stack
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator and Monitor.

Usage Guidelines

The `show stack` command is designed for debugging purposes, it should be used under the guidance of an HP Technical Support professional.

Examples

The following shows example output from the `show stack` command:

```
show stack
Stack Usage by Task
NAME          ENTRY          TID          SIZE    CUR    HIGH    MARGIN
-----
tExcTask      excTask      bfde18      7984    240    936     7048
tLogTask      logTask      bfb490      4984    224    1048    3936
tCrashDump    crashDumpTas 6b7bfc8     4080    160    224     3856
```

[Table 42](#) describes the significant fields in the display.

Table 42: Show Stack Field Descriptions

Field	Description
Name	The name of the task
Entry	The task entry point
TID	The task ID
Size	The maximum size of the task, in bytes
Cur	The current size of the task
High	The largest size of the task since the storage router was last started
Margin	The margin between the size of the task and the high

show system

To display a variety of system information about the storage router, including boot parameters and software versions, use the `show system` command. A table of information about HP SR2122-2 network interfaces also displays.

Syntax

```
show system
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show system` command to quickly display information about the storage router system configuration, including system name and model, current software version, date and time, NTP server, and name server information.

Examples

The following shows example output from the `show system` command:

```
show system
System Name: SR2122A
System Deployed for: SCSI routing
System Model: Sirocco
Disk Capacity: 30.50 Mbytes
Free Disk Space: 12.50 Mbytes
Software Version: 2.1.1
Last Reset: Tue Jul 17 13:41:49 CDT 2001
Current Time: Wed Jul 18 15:03:51 CDT 2001
Time Zone: US/Central
NTP Server: 10.1.60.86
Name Server: 10.1.40.243

Model              Number              Rev   Serial Number
System             SR2122-FCM-GEM      01    TAZ05030QBA
Processor          SIROCCO-E4          01    PAF05045AXY
Fibre Channel      FCM                 01    ZMG01030311
Gigabit Ethernet   GEM                 15    LAJ045208SG

Device  IP/Netmask      MAC
lo0     127.0.0.1/8     00:00:00:00:00:00
mgmt    10.1.10.244/24  00:01:44:60:f1:a0
ha      10.1.20.56/24  00:01:44:60:f1:a1
fc1
ge2
```

[Table 43](#) describes the significant fields in the display.

Table 43: show system Field Descriptions

Field	Description
System Name	The name of the storage router
System Model	The CPU type
Disk Capacity	Total size of the storage router disk
Free Disk Space	Total space available on the storage router disk
Software Version	The version of software that is currently running, such as 2.1.1
Last Reset	The date and time the system was last reset
Current Time	The current date and time

Table 43: show system Field Descriptions (Continued)

Field	Description
Time Zone	The time zone in which this storage router is located
NTP Server	The IP address of the time server
Name Server	The IP address of the primary and secondary DNS servers
Model Number	The model number for the storage router, processor, Fibre Channel and Gigabit Ethernet interfaces
Rev	The revision number for the storage router, processor, Fibre Channel and Gigabit Ethernet interfaces
Serial Number	The serial number for the storage router, processor, Fibre Channel and Gigabit Ethernet interfaces
Device	The name of the storage router interface
IP/Netmask	The IP address and network mask associated with the named interface
MAC	The machine address associated with the named interface

show task

To display information about tasks running in the storage router, issue the `show task` command.

Syntax

```
show task {all / taskid}
```

Table 44: Syntax Description

all	Keyword used to display information about all running tasks
taskid	The TID for a specific task, obtained from the <code>show task all</code> display or the <code>show system</code> display.

Defaults

None.

Command Modes

Administrator and Monitor.

Usage Guidelines

Use the `show task` command to view priority, status, and error information for all tasks, and to register and stack trace information for a specific task. The `show task` command is designed for debugging purposes, it should be used under the guidance of an HP Technical Support professional.

Examples

The following shows example output from the `show task all` command:

```
show task all
Running Tasks
NAME          ENTRY          TID      PRI  STATUS PC      SP
      ERRNO  DELAY
-----
---  ---  -----
tExcTask      excTask      bfde18   0    PEND  2cd38c  bfdd28
  3006b  0
tLogTask      logTask      bfb490   0    PEND  2cd38c  bfb3b0   0
  0
tCrashDump    crashDumpTas6 b7bfc8   0    PEND  275714  6b7bf28  0
  0
```


The following is example output from the `show task` command for TID *bfb490*:

```
show task bfb490
```

```
Registers
```

NAME	ENTRY	TID	PRI	STATUS	PC	SP	ERRNO
DELAY							
-----	-----	----	----	-----			
---	---	-----	-----				
tLogTask	logTask	bfb490	0	PEND	2cd38c	bfb3b0	0 0

```
stack: base 0xbfb490 end 0xbfa108 size 4984 high 1048 margin 3936
```

```
options: 0x6
```

```
VX_UNBREAKABLE VX_DEALLOC_STACK
```

```

r0  = 0          sp = bfb3b0      r2 = 0          r3 = 0
r4  = 0          r5 = 0          r6 = 0          r7 = 0
r8  = 0          r9 = 0          r10 = 0         r11 = 0
r12 = 0          r13 = 0          r14 = 0         r15 = 0
r16 = 0          r17 = 0          r18 = 0         r19 = 0
r20 = 310000     r21 = 310000     r22 = 300000    r23 = 310000
r24 = 310000     r25 = 310000     r26 = 310000    r27 = ffffffff
r28 = 10000003   r29 = 10000010   r30 = bfb6ac   r31 = 0
msr = b030      lr = 0   ctr = 0   pc = 2cd38c
cr  = 42000020  xer = 0

```

```
Stack Trace
```

```

2b3324 vxTaskEntry +60 : logTask ()
25c4e0 logTask +30 : msgQReceive ()
2743f0 msgQReceive +298: qJobGet ()

```

show tech-support

To display the results of several CLI show commands useful for debugging purposes, use the `show tech-support` command.

Syntax

```
show tech-support
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display the output of the following commands:

- `show system`
- `show clock`
- `show software version all`
- `show cluster`
- `show admin`
- `show interface brief`
- `show interface all`
- `show interface all stats`
- `show ip arp`
- `show ip hosts`
- `show ip route`
- `show ip tcp`
- `show ip udp`

- `show ip stats`
- `show ip icmp stats`
- `show ip route stats`
- `show ip tcp stats`
- `show ip udp stats`
- `show snmp`
- `show devices`
- `show accesslist all`
- `show scsirouter all`
- `show bootconfig`
- `show runningconfig`
- `show ha node stats`
- `show ha app list stats`
- `show ha app all stats`
- `show diagnostics`
- `show boot`
- `show memory`
- `show task all`
- `show stack`
- `show modules`
- `show buffers`
- `show debug scsirouter all testatus`
- `show debug fc all`

The `show tech-support` command is designed for debugging purposes, it should be used under the guidance of an HP Technical Support professional.

Examples

None.

show tech-support

CDP Commands

4

This section describes all the CLI commands related to CDP (Cisco Discovery Protocol). The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

cdp enable

To enable CDP on the SR 2122 Storage Router, use the `cdp enable` command.
To disable CDP on the storage router, use the `no` form of this command.

Syntax

```
cdp enable
no cdp enable
```

This command has no arguments or keywords.

Defaults

CDP is enabled.

Command Modes

Administrator.

Usage Guidelines

CDP is enabled by default to send or receive CDP information. CDP can be switched on or off for each specific interface. See the `cdp interface` command for more information.

Examples

The following example enables CDP on the storage router:

```
cdp enable
```

cdp holdtime

To specify the amount of time the receiving device should hold a CDP packet from the SR 2122 Storage Router before discarding it, use the `cdp holdtime` command. To revert to the default setting, use the `no` form of this command.

Syntax

```
cdp holdtime nn
no cdp holdtime
```

Table 45: Syntax Description

nn	Specifies the hold time to be sent in the CDP update packets, in seconds
----	--

Defaults

The default hold time is **180** seconds.

Command Modes

Administrator.

Usage Guidelines

The CDP hold time must be set to a higher number of seconds than the time between CDP transmissions, which is set using the `cdp timer` command.

Examples

The following example sets the CDP hold time to 60, meaning that the CDP packet being sent from the storage router should be held by the receiving device for 60 seconds before being discarded. You may want to set the hold timer lower than the default setting of **180** seconds if information about the storage router changes frequently.

```
cdp holdtime 60
```

cdp interface

To enable CDP for a specific interface, use the `cdp interface` command. To disable CDP for a specific interface, use the `no` form of this command.

Syntax

```
cdp interface ifname enable
no cdp interface ifname enable
```

Table 46: Syntax Description

ifname (?)	Specifies the name of the interface for which you are enabling or disabling CDP. CDP can be enabled on the mgmt (fei0), ha (fei1), and Gigabit Ethernet interfaces. When you type the <code>cdp interface ?</code> command, the CLI lists the interfaces available.
------------	---

Defaults

CDP is enabled for all interfaces.

Command Modes

Administrator.

Usage Guidelines

CDP must be enabled for the SR2122 Storage Router, using the `cdp enable` command, before it can be enabled for a specific interface.

Examples

The following example enables CDP for the Gigabit Ethernet interface, *ge2*:

```
cdp interface ge2 enable
```

The following example disables CDP for the management interface, *mgmt*:

```
cdp interface mgmt enable
```


cdp timer

To specify how often the HP SR2122-2 Storage Router sends CDP updates, use the `cdp timer` command. To revert to the default setting, use the `no` form of this command.

Syntax

```
cdp timer nn
no cdp timer
```

Table 47: Syntax Description

<i>nn</i>	Specifies the frequency with which the HP SR2122-2 Storage Router sends CDP updates, in seconds
-----------	---

Defaults

The default is **60** seconds.

Command Modes

Administrator.

Usage Guidelines

The time between CDP transmissions must be set to a lower number than the CDP hold time, which is set using the `cdp holdtime` command. There is a trade-off between sending more frequent CDP updates and bandwidth use.

Examples

The following example sets the CDP timer to *90*, meaning that CDP updates are sent every 90 seconds, which is less frequently than the default of **60** seconds. You might want to make this change if you are concerned about preserving bandwidth.

```
cdp timer 90
```

show cdp

To display global CDP configuration information for the storage router, including timer and hold-time information, use the `show cdp` command.

Syntax

```
show cdp
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

This command displays current CDP configuration. Use this command to determine if CDP is enabled, and to view packet timing and hold time information. CDP allows network applications, such as CiscoWorks, to learn device type information and the SNMP agent address of neighboring devices.

Examples

The following example displays CDP configuration information for the storage router. It shows that CDP is enabled and packets are sent every minute. The storage router directs its neighbors to hold its CDP advertisements for 3 minutes (the default CDP holdtime value). The storage router is also enabled to send CDP Version 2 advertisements.

```
show cdp
Global CDP information:
  CDP is enabled
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements are enabled
```

Table 48 describes the significant fields shown in the display.

Table 48: show cdp Field Description

Field	Definition
Sending CDP packets every nn seconds	The interval (in seconds) between transmissions of CDP advertisements. This field is controlled by the cdp timer command.
Sending a holdtime value of nn seconds	The amount of time (in seconds) the storage router direct neighbor to hold the CDP advertisement before discarding it. This field is controlled by the cdp holdtime command.
Sending CDPv2 advertisements are enabled	Indicates that CDP Version 2 advertisements are enabled.

show cdp entry

To display information about a specific neighboring device discovered using CDP, use the `show cdp entry` command.

Syntax

```
show cdp entry { * | all | device-id }
```

Table 49: Syntax Description

*	Displays all CDP neighbors
all	Displays all CDP neighbors
device-id	The CDP neighbor about which you want information. The user can also enter "*" which is the same as specifying all CDP neighbors.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display operational information about the storage router's CDP neighbors. Use `show cdp neighbors` command to display the device ID for the neighbor about which you want information.

Examples

The following shows sample output from the `show cdp entry` command. Information about all neighboring devices is displayed, including device ID, address and protocol, platform, interface, hold time, and version.

```
show cdp entry all
-----
Device ID: SCA0428017Q(msp-lab-sw1.hp.com)
Entry address(es):
IP address: 10.82.1.2
Platform: WS-C6509, Capabilities: Trans-Bridge Switch IGMP
Interface: mgmt, Port ID (outgoing port): 7/19
Holdtime : 176 sec

Version :
WS-C6509 Software, Version McpSW: 5.5(3) NmpSW: 5.5(3)
Copyright (c) 1995-2000 by
hp Systems
advertisement version: 2
VTP Management Domain: 'MSP-LAB'
Native VLAN: 210
Duplex: full
```

show cdp interface

To display information about the SR 2122 Storage Router interfaces on which Cisco Discovery Protocol (CDP) is enabled, use the `show cdp interface` command.

Syntax

```
show cdp interface [ifname]
```

Table 50: Syntax Description

<i>ifname</i>	Display CDP status and operational information for the specified storage router interface. The following are valid names: ha, mgmt, ge?.
---------------	--

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

CDP can be enabled for all storage router interfaces, including the management, high-availability, and Gigabit Ethernet interfaces. Use the `show cdp interface` command to display a brief summary of all storage router interfaces on which CDP is enabled. To display status and operational information for a specific interface, add the interface name argument.

Examples

The following shows example output from the `show cdp interface` command:

```
show cdp interface
Port    CDB Status
-----
mgmt     enabled
ha       enabled
ge2      enabled
```

The following is an example output for the management interface (mgmt):

```
show cdp interface mgmt
show cdp interface mgmt
Port    CDB Status
-----
mgmt     enabled
```

show cdp neighbors

To display detailed information about neighboring devices discovered using CDP, use the `show cdp neighbors` command.

Syntax

```
show cdp neighbors [interface ifname] [detail]
```

Table 51: Syntax Description

<code>interface ifname (?)</code>	Keyword and name of the storage router interface connected to the neighbors about which you want information. (Optional)
<code>detail</code>	Displays detailed information about a neighbor (or neighbors) including network address, enabled protocols, hold time, and software version. (Optional)

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show cdp neighbors` command to display either brief or detailed information about neighboring devices discovered using CDP. Add the **interface** keyword and the interface name to limit the display to neighbors connected to that specific interface.

Use the **detail** keyword to display detailed information about all devices or about devices connected to te specific interface.

Examples

The following is an example output from the `show cdp neighbors` command:

```
show cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge

                  S - Switch, H - Host, I - IGMP, r - Repeater
Local-Port      Device-ID      Capability  Platform  Port-ID
-----
mgmt            SCA0428017Q    T S I      WS-C6509   7/19
```

Table 52 describes the significant fields shown in the display.

Table 52: show cdp Neighbors Field Description

Field	Description
Capability Codes	The type of device that can be discovered
Local-Port	The name of the local interface. mgmt is the management interface, ha is the HA interface, and ge? is the Gigabit Ethernet interface.
Device-ID	The name of the neighbor device and either the MAC address or the serial number of this device
Capability	The type of the device listed in the CDP Neighbors table. Possible values are: R—Router T—Transparent bridge B—Source-routing bridge S—Switch H—Host I—IGMP device r—Repeater
Platform	The product number of the device
Port-ID	The protocol and port number of the device

The following is a sample output for one neighbor from the **show cdp neighbors detail** command. The output includes additional information about the neighbor, including network address, enabled protocols, and software version.

```
show cdp neighbors detail
-----
Device ID: SCA0428017Q(msp-lab-sw1.hp.com)
Entry address(es):
IP address: 10.82.1.2
Platform: WS-C6509, Capabilities: Trans-Bridge Switch IGMP
Interface: mgmt, Port ID (outgoing port): 7/19
Holdtime : 153 sec

Version :
WS-C6509 Software, Version McpSW: 5.5(3) NmpSW: 5.5(3)
Copyright (c) 1995-2000 by HP Systems

advertisement version: 2
VTP Management Domain: 'MSP-LAB'
Native VLAN: 210
Duplex: full
```


Table 53 describes the significant fields shown in the display.

Table 53: show cdp neighbors Field Description

Field	Description
Device-ID	The name of the neighbor device and either the MAC address or the serial number of this device
Entry address(es)	A list of network addresses of neighbor devices
network protocol address	The network address of the neighbor device. The network address in the example output is an IP address.
IP address	The IP address of the neighboring devices
Platform	The product number of the device
Capability	The device type of the neighbor. This device can be a router, a bridge, a transparent bridge, a source-routing bridge, a switch, a host, an IGMP device, or a repeater.
Interface	The protocol and port number of the port on the current device
Holdtime	The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it.
Version	The software version of the neighbor device
advertisement version	The CDP advertisement version
Duplex	The duplex state of connection between the storage router and the neighbor device
sysObject ID	The system object identifier

show cdp traffic

To display information about traffic between devices gathered using CDP, use the `show cdp traffic` command.

Syntax

```
show cdp traffic
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to view statistics about CDP traffic between the storage router and other devices.

Examples

The following is an example output from the `show cdp traffic` command.

```
show cdp traffic
CDP counters :
  Total packets output: 2530, Input: 1262
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 0, Input: 0
  CDP version 2 advertisements output: 2530, Input: 1262
```

Table 54 describes the significant fields shown in the display.

Table 54: show cdp traffic Field Descriptions

Field	Description
Total packets output	The number of CDP advertisements sent by the storage router. This value is the sum of the CDP Version 1 advertisements output and CDP Version 2 advertisements output fields.
Input	The number of CDP advertisements received by the storage router. This value is the sum of the CDP Version 1 advertisements input and CDP Version 2 advertisements input fields.
Hdr syntax	The number of CDP advertisements with bad headers received by the storage router
Chksum error	The number of times the verification operation failed on incoming CDP advertisements
Encaps failed	The number of times CDP failed to send advertisements on an interface because of a failure caused by the bridge port of the storage router.
No memory	The number of times the storage router did not have sufficient memory to store the CDP advertisements in the advertisement cache table when the storage router was attempting to assemble advertisement packets for transmission and parse them when receiving them.
Invalid packet	The number of invalid CDP advertisements received and sent by the storage router
Fragmented	The number of times fragments or portions of single CDP advertisements were received by the storage router instead of the complete advertisement.
CDP version 1 advertisement s output	The number of CDP Version 1 advertisements sent by the storage router
Input	The number of CDP Version 1 advertisements received by the storage router
CDP version 2 advertisement s output	The number of CDP Version 2 advertisements sent by the storage router.
Input	The number of CDP Version 2 advertisements received by the storage router

show cdp traffic

Clock Commands

5

This section describes all the CLI commands related to the clock setting and monitoring function in the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

clock set

To set the storage router system clock to the given date and time, use the `clock set` command. Date and time information is used for log files and the user interface.

Syntax

`clock set hh:mm:ss month day year`

Table 55: Syntax Description

<code>hh:mm:ss</code> <code>month day</code> <code>year</code>	The current time, in hours, minutes, and seconds, followed by the current month, day and year. For example, 13:55:22 06 22 2001.
--	--

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

If the storage router should synchronize its date and time with a network time protocol (NTP) server, see the `ntp peer` command.

Examples

The following example sets the storage router date and time to June 22, 2001 at 14:39:00.

```
clock set 14:39:00 06 22 2001
```

clock timezone

To set the time zone for the storage router, use the `clock timezone` command.

Syntax

```
clock timezone zone
```

Table 56: Syntax Description

zone (?)	A character string representing the time zone of the storage router. For example, "America/Chicago" or "Europe/Amsterdam."
----------	--

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Unless you set the time zone, the clock setting is assumed to be in Universal Time (GMT).

You can use the **setup time** wizard to select a time zone, set the clock and date, and identify an NTP server for the storage router.

To use the `clock timezone` command, you must know the appropriate time zone string. Use the "?" to display a list of valid time zone strings. For example, "`clock timezone US?`" displays only US time zones.

Examples

The following example sets the storage router time zone to US/Mountain:

```
clock timezone US/Mountain
```

ntp peer

To set the name or IP address of a Network Time Protocol (NTP) server with which the storage router will synchronize date and time, use the `ntp peer` command. To clear the current NTP server setting, use the `no` form of this command.

Syntax

```
ntp peer {A.B.C.D | servername}  
no ntp peer
```

Table 57: Syntax Description

A.B.C.D	The IP address of the NTP server with which the storage router synchronizes date and time. A.B.C.D is the dotted quad notation of the IP address. If the first character is a valid digit [0-9] then the parser assumes the user entered an IP address.
servername	The name of the NTP server with which the storage router synchronizes date and time. In order to specify a server name, the storage router must be configured to use DNS server using the <code>ip name-server</code> command. If the first character is not a valid digit [0-9] then the parser assumes the user entered a server name.

Defaults

None.

Command Modes

Administrator

Usage Guidelines

The storage router must provide accurate date and time information for log files and user interfaces. It will use the services of the NTP server to keep the date and time synchronized with the rest of the network.

If the NTP server is outside the storage router management subnet, use the `ip route` command to add an appropriate gateway IP address to the HP SR2122-2 routing table.

Examples

The following example sets the address of the NTP server for the SR 2122 to *10.1.60.86*.

```
ntp peer 10.1.60.86
```

show clock

To display the current system date and time, use the `show clock` command. The information displays in the following format:

Syntax

```
show clock
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display the storage router date and time setting.

Examples

The following is an example output from the `show clock` command:

```
show clock
Wed Jul 11 15:22:00 CDT 2001
```

show clock

Configuration Commands

6

This section describes all the CLI commands related to setting and showing the configuration of the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

delete savedconfig

To show or remove the named file(s) from the `savedconfig` directory, use the `delete savedconfig` command.

Syntax

```
delete savedconfig
delete savedconfig file
delete savedconfig all
```

Table 58: Syntax Description

<code>file</code>	The name of the configuration file to be deleted. This file must exist in the <code>savedconfig</code> directory (Optional)
<code>all</code>	Keyword, indicating that all configuration files in the <code>savedconfig</code> directory will be deleted (Optional)

Defaults

The default is to show all the configuration files that can be deleted in the `savedconfig` directory.

Command Modes

Administrator.

Usage Guidelines

Use the `show savedconfig` command to display the contents of the `savedconfig` directory.

Examples

The following example removes the configuration file named `foo_config` from the storage router:

```
delete savedconfig foo_config
```

restore aaa

To copy AAA authentication methods from the specified configuration file into persistent memory, use the `restore aaa` command. The configuration file must exist in the `savedconfig` directory. To display the contents of the `savedconfig` directory, execute the `show savedconfig` command.

Syntax

```
restore aaa from file
```

Table 59: Syntax Description

from <i>file</i>	The name of the configuration file containing the information to be restored. This file must exist in the <code>savedconfig</code> directory.
-------------------------	---

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `restore` command overwrites all existing AAA configuration information, including any user names and passwords in the local username database, RADIUS and TACACS+ configuration information, and the default AAA authentication list used for iSCSI authentication.

Examples

The following example restores the AAA authentication methods from the saved configuration file named *aaa_backup*:

```
restore aaa from aaa_backup
```

restore accesslist

To copy the named access list (or all access lists) from the specified configuration file into persistent memory, use the `restore accesslist` command. The configuration file must exist in the `savedconfig` directory. To display the contents of the `savedconfig` directory, issue the `show savedconfig` command.

Note: If the storage router belongs to a cluster, the restored access list information will automatically be propagated to other members of that cluster.

Syntax

```
restore accesslist {name / all} from file
```

Table 60: Syntax Description

<code>name</code>	The name of the access list to be restored
<code>all</code>	Keyword to restore all access lists
<code>from file</code>	The name of the configuration file containing the information to be restored. This file must exist in the <code>savedconfig</code> directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

If the access list currently exists in some form, the `restore` command does not delete existing information. The `restore` command adds missing entries or overwrites existing entries of the same name, but it never purges or deletes existing access list entries. If necessary, you can delete an access list and all its entries and then restore it from a saved configuration file.

Note: In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the `restore accesslist` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions.

Examples

The following example restores the access list named *fooList* from the saved configuration file named *accessList_backup*:

```
restore accesslist fooList from accessList_backup
```

restore all

To copy all the previously saved configuration information from the specified configuration file into persistent memory, use the `restore all` command. The configuration file must exist in the `savedconfig` directory. Use the `show savedconfig` command to display the contents of the `savedconfig` directory.

Note: This command does not change the running configuration of the storage router.

Syntax

```
restore all from file
```

Table 61: Syntax Description

<code>all</code>	Keyword indicating that all access lists and vlans, and all instances of SCSI routing services within the named configuration file will be restored.
<code>from file</code>	The name of the configuration file containing the information to be restored. This file must exist in the <code>savedconfig</code> directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `restore all` command restores all information from the named configuration file. Depending on the information that is restored, the running configuration of the storage router will be changed.

A `restore` command may overwrite or delete existing items. However, the `restore` command will not purge or delete existing items from access lists, but will add missing items or overwrite existing items of the same name. If necessary, you can delete access lists, or any other item to be restored, before restoring from a saved configuration file.

SCSI routing instances must be stopped before they can be restored. Use the `no scsirouter enable` command to stop active SCSI routing instances.

Note: In a cluster environment, all access lists and VLANs must be created and maintained on the first storage router to join the cluster. If you issue the `restore all` command from another storage router in the cluster, any saved access lists or VLAN will not be restored. The CLI displays an informational message with the IP address of the storage router that is currently handling all access list and VLAN functions.

Examples

The following example restores all configuration data contained in the configuration file named *foo_backup* into persistent memory:

```
restore all from foo_backup
```


restore scsirouter

To copy the previously saved configuration information related to the named SCSI routing instance (or all instances) from the specified configuration file into persistent memory, use the `restore scsirouter` command. The configuration file must exist in the `savedconfig` directory. Use the `show savedconfig` command to display the contents of the `savedconfig` directory.

Note: This does not change the running configuration.

Syntax

```
restore scsirouter {name | all} from file
```

Table 62: Syntax Description

name	The name of the SCSI routing instance to be restored
all	Keyword to restore all SCSI routing instances
from file	The name of the configuration file containing the information to be restored. This file must exist in the <code>savedconfig</code> directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

A SCSI routing instance must be inactive before it can be restored. Use the `no scsirouter enable` command to stop an active SCSI routing instance so it can be restored. After the specified SCSI routing instance is restored, issue the `scsirouter enable` command to start the instance and update the storage router's running configuration.

A `restore` command never deletes existing SCSI routing instances. The `restore` command adds missing instances and overwrites configuration information for existing instances of the same name. If necessary, you can delete a SCSI routing instance and then restore it from a saved configuration file.

Examples

The following example restores the SCSI routing instance *foo1* from the configuration file named *scsi_backup001*:

```
restore scsirouter foo1 from scsi_backup001
```

restore system

To copy the previously saved configuration information from the specified configuration file into persistent memory, use the `restore system` command. The configuration file must exist in the `savedconfig` directory. Use the `show savedconfig` command to display the contents of the `savedconfig` directory.

Note: This does not change the running configuration.

Syntax

```
restore system all from file  
restore system {cdp | contactinfo | ip-route | logging |  
name-server | ntp | remotelog | restrict | snmp | software |  
telnet} from file
```

Table 63: Syntax Description

<code>cdp</code>	Restore CDP configuration information
<code>contactinfo</code>	Restore administration contact information
<code>ip-route</code>	Restore static ip route information
<code>logging</code>	Restore logging facility configuration information
<code>name-server</code>	Restore DNS configuration information
<code>ntp</code>	Restore NTP server configuration information
<code>remotelog</code>	Restore remote logging configuration information, including the syslog host and the syslog facility
<code>restrict</code>	Restore the storage router restrict configuration
<code>snmp</code>	Restore SNMP configuration information
<code>software</code>	Restore the default software download location, user name and password information for HTTP, proxy, and TFTP
<code>telnet</code>	Restore telnet configuration information
<code>all</code>	Restore all restorable system information from saved configuration file. Restorable system information includes CDP configuration, administrator contact data, DNS and NTP information, restrict configuration, remote login data, and the default download location for updated storage router software.
<code>from file</code>	The name of the configuration file containing the information to be restored. This file must exist in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Some system information that is saved when the `save system` command is issued is not available for restoration from a saved configuration file. Use the `show savedconfig` command to display the contents of the specified configuration file. The following information is available for display but cannot be restored:

- Management and HA interface IP addresses
- Fibre Channel and Gigabit Ethernet interface configuration information
- Administrator mode and Monitor mode passwords
- HA configuration mode

Examples

The following example restores all restorable system configuration information from the saved configuration file `scsi_backup_0524`:

```
restore system all from scsi_backup_0524
```

restore vlan

To copy the specified VLAN from the named configuration file into persistent memory, use the `restore vlan` command. The configuration file must exist in the `savedconfig` directory. To display the contents of the `savedconfig` directory, issue the `show savedconfig` command.

Syntax

```
restore vlan {all | vid} from file
```

Table 64: Syntax Description

all	Keyword used to restore all VLAN definitions
vid	The VLAN identification number
from file	The name of the configuration file containing the information to be restored. This file must exist in the <code>savedconfig</code> directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

If the VLAN currently exists, the `restore vlan` command overwrites existing configuration information with the information from the named configuration file. The `restore vlan` command also sets the VTP configuration information.

In a cluster environment, all VLANs must be created and maintained on the first storage router to join the cluster. If you issue the `restore vlan` command from another storage router in the cluster, any saved VLANs will not be restored. The CLI displays an informational message with the IP address of the storage router that is currently handling all VLAN functions.

Examples

The following example restores VLAN *100* from the *vlanBackup* file:

```
restore vlan 100 from vlanBackup
```

save aaa

To save the current AAA settings to non-volatile memory, use the `save aaa` command.

Syntax

```
save aaa bootconfig  
save aaa filename
```

Table 65: Syntax Description

bootconfig	Keyword, indicating the AAA settings to the storage router's bootable configuration, which is used when the HP SR2122-2 Storage Router is restarted
filename	The name of the file where the AAA configuration information will be written. This file is stored in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You must save configuration data from the running configuration to the boot configuration file for it to be retained in the storage router when it is restarted. Use the *filename* parameter to save the AAA configuration to a file. Configurations copied to a file can be moved between storage routers and can be restored at a later time.

The following information is saved:

- The AAA authentication list
- The username database
- All RADIUS server configuration information
- All TACACS+ server configuration information

Examples

The following example copies the running AAA settings to the bootable configuration, used when the storage router is restarted:

```
save aaa bootconfig
```

The following example copies the running AAA settings to a file named *aaa_SR2122A*:

```
save aaa aaa_SR2122A
```

save accesslist

To save configuration data for the named accesslist or for all access lists to non-volatile memory, use the `save accesslist` command.

Syntax

```
save accesslist {name / all} bootconfig
save accesslist {name / all} filename
```

Table 66: Syntax Description

name (?)	The name of the access list to be copied
all	Keyword, indicating all access lists associated with this storage router will be saved
bootconfig	Keyword, indication the access list from the running configuration will be saved to the system bootable configuration, used when the SR 2122 Storage Router is restarted
filename	The name of the file where the running access list configuration data will be written. This file is stored in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

Note: In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the `save accesslist` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions.

Examples

The following example saves the current configuration for all access lists to the bootable configuration, used when the storage router is restarted:

```
save accesslist all bootconfig
```

The following example saves the access list *fooList* to a configuration file named *fooList_SR2122A*:

```
save accesslist all fooList_SR2122A
```

save all

To save all configuration data for a storage router to non-volatile memory, use the `save all` command.

Syntax

```
save all bootconfig
save all filename
```

Table 67: Syntax Description

bootconfig	Keyword indicating that the current running configuration information will be saved to the bootable configuration, used when the SR 2122 Storage Router is restarted
filename	The name of the file where the configuration data will be written. This file is stored in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted.

Depending on the storage router deployment, the `save all` command saves AAA configuration, SCSI routing instances, or FC server instances, access lists, VLANs and selected system configuration. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

Note: In a cluster environment, all access lists and VLANs must be created and maintained on the first storage router to join the cluster. If you issue the `save all` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list and VLAN functions.

Examples

The following example saves the current running configuration to the bootable configuration, used when the storage router is restarted:

```
save all bootconfig
```

The following example copies the current running configuration to the file named `SR2122A_03Nov2001`. You may want to do this as a means of archiving the current running configuration of the storage router on a regular basis.

```
save all SR2122A_03Nov2001
```

save fc-server

To save all configuration data associated with the named FC server instance to non-volatile memory, use the `save fc-server` command.

Syntax

```
save fc-server {name / all} {bootconfig / filename}
```

Table 68: Syntax Description

name	The name of the FC server instance
all	Save configuration data for all FC server instances
bootconfig	Save the FC server instance from the running configuration to the storage router's bootable configuration, used when the SR 2122 Storage Router is restarted
filename	The name of the file where the configuration data will be written. This file is stored in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

Examples

The following example saves the FC server instance *defaultFC* currently running on this storage router to the bootable configuration, used when the storage router is restarted:

```
save fc-server defaultFC bootconfig
```

save scsirouter

To save all configuration data associated with the named SCSI routing instance or all instances to non-volatile memory, use the `save scsirouter` command.

Syntax

```
save scsirouter {name | all} bootconfig
save scsirouter {name | all} filename
```

Table 69: Syntax Description

name (?)	The name of the SCSI routing instance
all	Keyword, indicating that configuration data for all SCSI routing instances will be saved
bootconfig	Keyword, indicating the SCSI routing instance from the running configuration will be saved to the bootable configuration, used when the SR 2122 Storage Router is restarted
filename	The name of the file where the configuration data will be written. This file is stored in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is started. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

In a cluster environment, a storage router that is currently running a SCSI routing instance is known as the current primary for that instance. The SCSI routing instance can only be saved on the storage router that is the current primary for that instance.

Examples

The following example saves all SCSI routing instances currently running on this storage router to the bootable configuration, which is used when the storage router is restarted:

```
save scsirouter all bootconfig
```

The following example saves the SCSI routing instance named *foo* to the file named *foo_SR2122A*:

```
save scsirouter foo foo_SR2122A
```

save system

To save all selected system configuration information to non-volatile memory, use the `save system` command.

Syntax

```
save system bootconfig
```

```
save system filename
```

Table 70: Syntax Description

bootconfig	Keyword, indicating the current running system configuration will be saved to the bootable configuration, used when the SR 2122 Storage Router is restarted
filename	The name of the file where the system configuration data will be written. This file is stored in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and selected items can be restored at a later time.

The following system configuration data is saved:

- Monitor and Administrative passwords
- Administrative contact information
- Network Time Protocol (NTP) server name
- Primary and optional secondary Domain Name Server (DNS)
- Default location for downloading SR 2122 software
- System name
- Logging facility information
- Management and high availability (HA) interface addresses
- Static routes
- SNMP settings
- CDP settings
- Restrict settings
- Remote logging settings

Examples

The following example saves the current system configuration to the bootable configuration, used when the storage router is restarted:

```
save system bootconfig
```

The following example saves the current system configuration to the file named *sys_SR2122A*:

```
save system sys_SR2122A
```

save vlan

To save all VLAN and VTP configuration information for the specified VLAN or for all VLANs to non-volatile memory, use the `save vlan` command.

Syntax

```
save vlan {all / <vid>} bootconfig
save vlan {all / <vid>} filename
```

Table 71: Syntax Description

vid	The VLAN identification number of the VLAN configuration to be saved
all	Save all VLANs associated with this storage router
bootconfig	Keyword, indicating the current VLAN configuration will be saved to the bootable configuration, used when the Storage Router is restarted
filename	The name of the file where the current VLAN configuration data will be written. This file is stored in the savedconfig directory.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

VTP mode and domain information is saved along with the specified VLAN configuration information.

Examples

The following example saves the current VLAN configuration for all VLANs to the system's bootable configuration, which is used when the storage router is restarted:

```
save vlan all bootconfig
```

The following example saves VLAN 12 to the file named *vlan_SR2122A*:

```
save vlan 12 vlan_SR2122A
```

show boot

To display system boot information and startup file parameters, use the `show boot` command.

Syntax

```
show boot
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to view system boot information such as the boot device type, path to the boot image, and path to the file containing the startup commands. The `show boot` command is designed for debug purposes and should be used under the guidance of an HP Technical Support professional.

Examples

The following example displays system boot information:

```
show boot
Boot Device: ide-0,00
Boot File: /ata0/vxWorks
Startup File: /ata0/NuSpped.start
Flags: 0x0
Target Name: SR2122A
Target IP: 10.1.10.205:ffffff00
Booted From:
Booted From IP:
Gateway IP:
User Name:
Password:
```

show bootconfig

To display the bootable configuration for the storage router, or save the commands used to create the bootable configuration to a file, use the `show bootconfig` command.

Syntax

```
show bootconfig
show bootconfig from filename
show bootconfig to filename
```

Table 72: Syntax Description

<i>from filename</i>	Display the bootable configuration information from the specified configuration file. The file is stored in the savedconfig directory (Optional)
<i>to filename</i>	Save bootable configuration as a series of CLI commands to the specified file. The file will be saved in the script directory. (Optional)

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

- Use the **from** keyword to display the bootable configuration information stored in the specified configuration file.
- Use the **to** keyword to save the bootable configuration as a series of CLI-like commands in the specified file. The file is saved in the `script` directory and can be used as a starting point to recreate an existing storage router bootable configuration using the `read script` command.
- Only bootconfig elements that actually contain information are displayed. Items that have not yet been given a configuration value may not be displayed.

Table 73: Show bootconfig elements

Element	Description
AAA	The authentication, authorization and accounting method configuration information
Accesslist	The access list description and entry information
Admin	The storage router administrator contact information
Admin Login	The Administrator mode password
CDP	The Cisco Discovery Protocol configuration including timer and hold time settings
Cluster	The name of the cluster to which this storage router belongs
DNS	The name of any defined domain name servers
FC?	The operational characteristics of the Fibre Channel interface(s) and user port information, if present
GE?	The IP address and operational characteristics of the Gigabit Ethernet interface
HA	The HA configuration information
HA Port	The IP address and operational characteristics of the HA interface
Logging Route Facility	The configuration information for the logging facility
MGMT Port	The IP address and operational characteristics of the management interface

Table 73: Show bootconfig elements (Continued)

Element	Description
Monitor Login	The Monitor mode password
Remote Log	The remote Logging configuration information
Restrict	The storage router interface restrictions
Routes	The configuration information for default gateway and so on
Scsirouter	The configuration information for each SCSI routing instance or FC server instance, including name, description, server interface, and other instance specific configuration information
Software	The default download location for the storage router software
SNMP	The SNMP settings
SNTP	The date and time information, including the address of any associated NTP server
SYSTEM	The specific system information, such as hostname
Telnet	The telnet session timeout information
VLAN	The virtual LAN configuration information
VTP Domain	The VTP domain name
VTP Mode	The VTP configuration mode

Examples

The following example creates a script file named *initial_SR2122A* in the *script* directory which contains the output from the `show bootconfig` command:

```
show bootconfig to initial_SR2122A
```

The following example displays the storage router configuration from the bootable configuration.

```
show bootconfig
!
! CLUSTER
!
cluster 3d000120
!
! ACCESSLIST
!
accesslist y
!
accesslist xx
!
accesslist x
!
! VTP DOMAIN
!
vtp domain none
!
! VTP MODE
!
vtp mode client
!
!
! VLAN
! (no vlan(s) found)
!
! SCSIROUTER
!
scsirouter bob
scsirouter bob description "toms"
scsirouter bob authentication "none"
scsirouter bob primary "none"
scsirouter bob target naming authority "xx"
scsirouter bob reserve proxy disable
scsirouter bob target xx enabled
scsirouter bob target xx accesslist "none"
scsirouter bob target xx loopid "2"
!
scsirouter x
scsirouter x authentication "none"
scsirouter x primary "none"
scsirouter x target naming authority "none"
scsirouter x reserve proxy disable
```

```
!  
scsirouter xx  
scsirouter xx authentication "none"  
scsirouter xx primary "none"  
scsirouter xx target naming authority "none"  
scsirouter xx reserve proxy disable  
!  
scsirouter xxxx  
scsirouter xxxx authentication "none"  
scsirouter xxxx primary "xxx"  
scsirouter xxxx target naming authority "none"  
scsirouter xxxx reserve proxy disable  
!  
! FEI0 (Mgmt Port)  
!  
interface mgmt ip-address 10.1.30.60/255.255.255.0  
!  
! FEI1 (HA Port)  
!  
interface ha ip-address 10.1.29.2/255.255.255.0  
!  
! FC1  
!  
interface fc1 mtusize 65280  
interface fc1 topology ptppref  
!  
! GE2  
!  
interface ge2 mtusize 1500  
interface ge2 autonegotiation autodetect  
!  
! ADMIN  
!  
admin contactinfo email t  
!  
! SNTP  
!  
clock timezone US/Samoa  
!  
! SNMP  
!  
snmp-server getcommunity public ro  
snmp-server setcommunity private rw  
snmp-server host 10.1.29.5 traps  
!
```

```

! DNS
!
! (none)
!
! SOFTWARE
!
software http url http://www.hp.com
!
! CDP
!
no cdp enable
cdp timer 254
cdp holdtime 10
!
! AAA
!
aaa new-model
username friday password <password>
username yy password <password>
username x password <password>
username xyz password <password>
username xggg password <password>
username qqqq password <password>
username ccc password <password>
username ww password <password>
username www password <password>
radius-server key <key>
radius-server timeout 12
radius-server retransmit 2
radius-server host 5.6.7.8 auth-port 12 timeout 12 retransmit 12
radius-server host 1.2.3.4 auth-port 1645 timeout 12 retransmit 13
radius-server host 1.2.3.4 auth-port 12 timeout 1 retransmit 1
tacacs-server key <key>
tacacs-server timeout 22
tacacs-server host 1.2.2.3 auth-port 12 timeout 1
tacacs-server host 1.2.3.3 auth-port 7 timeout 1
tacacs-server host 1.2.3.3 auth-port 12 timeout 1

```

show runningconfig

To display the current running configuration of the storage router or save the commands used to create the running configuration to a file, use the `show runningconfig` command.

Syntax

`show runningconfig to filename`

Table 74: Syntax Description

filename	Save the storage router's running configuration as a series of CLI commands specified in a file. The file is stored in the script directory (Optional)
----------	--

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show runningconfig` command to display the current system configuration information as it would be saved to a configuration file. Use the **to** keyword to save the running configuration as a series of CLI-like commands in the specified file. This file is saved in the `script` directory and can be used as a starting point to recreate the existing storage router running configuration, using the `read script` command.

Example

The generated output format and content is the same as for the `show bootconfig` command.

show savedconfig

To list the available files in the `savedconfig` directory or to view the contents specific configuration file, use the `show savedconfig` command. Configuration files are stored in the `savedconfig` directory.

Syntax

```
show savedconfig file
```

Table 75: Syntax Description

<i>file</i>	The name of the configuration file to display. This file must exist in the <code>savedconfig</code> directory. (Optional)
-------------	---

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display a list of configuration files in the `savedconfig` directory before attempting a restore. Use the *file* parameter to view the contents of the specified configuration file. You can also use the `show scsirouter` from or `show accesslist` from commands to display specific objects from the named configuration file, allowing you to verify that the object of your `restore` command exists in the selected file.

The generated output format is the same as for the `show bootconfig` | `runningconfig` command.

Examples

The following is example output from the `show savedconfig` command:

```
show savedconfig
bootconfig
Config-Jul172001
MyConfig.xml
Config-Jul242001
```

The following is example output from the `show savedconfig` command using the *file* parameter:

```
show savedconfig bootconfig
scsirouter red description "(not set)"
scsirouter RAID description "(not set)"
scsirouter blue description "(not set)"
scsirouter black description "(not set)"
scsirouter brown description "(not set)"
scsirouter green description "(not set)"
scsirouter orange description "(not set)"
scsirouter purple description "(not set)"
scsirouter yellow description "(not set)"
scsirouter ht-dataver description "(not set)"
scsirouter oracle-sun description "(not set)"
scsirouter oracle-sunfs description "(not set)"
```


Fibre Channel Port Commands



This section describes all the CLI commands related to the external Fibre Channel and SCSI ports in the system. Note that a parallel SCSI interface is currently not available on any storage router product. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

interface fci? mode

To set the interface mode for the specified internal Fibre Channel (FC) interface, use the `interface fci? mode` command.

```
interface fci? mode {fcip | scsirouter}
```

Table 76: Syntax Description

fci?	The name of the internal FC interface. Valid values are <code>fci1</code> or <code>fci2</code> . When you type the interface fci? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
fcip	Enable the interface for FCIP.
scsirouter	Enable the interface for SCSI routing.
transparent-dynamic	Enable the interface for transparent SCSI routing, deployed in dynamic mode.
transparent-static	Enable the interface for transparent SCSI routing, deployed in static mode.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

Use the **interface fci? mode** command to manually deploy the storage router for mixed mode support. When the storage router is deployed for mixed mode, one internal FC interface is configured to support SCSI routing or transparent SCSI routing, and the other internal FC interface is configured to support FCIP.

When the storage router is deployed for SCSI routing or transparent SCSI routing, one internal FC interface can be configured to support FCIP. When the storage router is deployed for FCIP, one internal FC interface can be configured to support SCSI routing.

To change the deployment option for a storage router deployed for SCSI routing without clearing the system configuration, reconfigure both internal FC interfaces for FCIP, and delete all SCSI routing instances. To change the deployment option for a storage router deployed for FCIP without clearing the system configuration, reconfigure both internal FC interfaces for SCSI routing, and delete all FCIP instances.

Use the **show system** command to see the current system deployment for the storage router.

Note: You must save the configuration change and reboot the storage router for the mode change to take effect.

Examples

The following example enables the *fcil* interface for SCSI routing, saves the storage router bootable configuration and reboots the system:

```
[HP SR2122-2]# interface fcil mode scsirouter
```

Related Commands

Command	Description
<code>show system</code>	Display selected system information, including deployment mode.

interface fc? topology

To set port topology on a Fibre Channel interface, use the `interface fc? topology` command. This command is not applicable when the storage router is deployed for transparent SCSI routing.

Syntax

```
interface fc? topology {loop / looppref / ptp}
```

Table 77: Syntax Description

loop	Keyword, indicates the port will only support arbitrated loop topology. This setting is recommended when connecting to Fibre Channel hubs.
looppref	Keyword, indicates the port will support either arbitrated loop or point to point topology. The port will attempt to come up in arbitrated loop mode but will fall back to point to point mode. This is the default setting when connecting to a Fabric Switch.
ptp	Keyword, indicates port will only support point to point topology. This setting should only be used when connecting to a Fabric Switch.

Defaults

By default the port topology is set to *loop* when the setup script is configured for connection to a Fibre Channel hub and set to *looppref* when the setup script is configured for connection to a Fabric Switch. The port topology is forced to *loop* when the storage router is deployed for transparent SCSI routing.

Command Modes

Administrator.

Usage Guidelines

Allows the user to set the port topology on a specified Fibre Channel interface.

Examples

The following example sets the port topology to point to point on the Fibre Channel interface *fc2*.

```
interface fc2 topology ptp
```

show debug fc?

To display a variety of debug information for the specified SCSI router services instance or target and LUN combination, use the `show debug fc?` command.

Syntax

```
show debug lldrestartfcfw fc?
show debug forcefcfwdump fc?
show debug rawlundatabase fc?
show debug mailboxtrace fc?
```

Table 78: Syntax Description

lldRestartfcfw	Keyword to restart the Fibre Channel firmware. Any existing connections may be dropped.
forcefcfwdump	Keyword to force a dump of firmware. A file named qlclifwdump0?.txt is created where ? is the Fibre channel interface being dumped.
rawlundatabase	Keyword used to display raw LUN database information for all discovered targets.
mailboxtrace	Keyword used to display a logic mailbox trace information in hex.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

To enable trace facilities for debugging SCSI routing instances, use the `debug scsirouter` command.

The `show debug` command is designed for debug purposes, and should only be used under the guidance of a HP Technical Support professional.

Examples

The following is example output from the `show debug rawlunatabase fc1` command:

```
show debug rawlunatabase fc1
Entry Address = 0xd442b6c
fabricLoginFailureCode=0x0,fabricLoginExtendedCode=0x0,fabricLogin
TimeoutCode=0x0
ReportLunsLLDStatus=0x0,ReportLunsLLDStatusModifier=0x0,ReportLuns
SCSIStatus=0x0,ReportLunsASCASCQ=0x0,ReportLunsLunCount=1
InquiryLLDStatus=0x0,InquiryLLDStatusModifier=0x0,InquiryLastLunWi
thLLDError=0x0,
InquirySCSIStatus=0x0,InquiryASCASCQ=0x0,InquiryLastLunWithSCSISa
tusError=0x0
boolLunsNotSupported=0x0,InquiryLastLunNotSupported=0x0
loopId=0x0,masterState=0x6,slaveState=0x7,loggedIn=1,roles=1,valid
=1,portId=0x102e1,scanLuns=0x0
numberLuns=0x1,reportAsyncEvent=0x0,node_wwn=0x20000020
0x37c59d28, port_wwn=0x21000020 0x37c59d28

lun=0, wwnn=0x20000020 0x37c59d28, reportAsyncEvent=0x0
stdInquiry data for lun=0x0
bytes0-7=0x00000332 0x8b00500a
vendorId=SEAGATE , product=ST318451FC, revision=0001 device
Type=0x0
DeviceIdPage:bytes0-3= 0x0083000c,bytes4-7= 0x01030008,bytes8-11=
0x20000020
:bytes12-15=
0x37c59d28,bytes16-19=0x00800014,bytes20-23=0x33434330
S/N Page:bytes0-3= 0x00800014 s/n=3CC05V5Z00007116DSRB
```

show debug interface fc?

To display debug information for internal Fibre Channel (FC) interface switch ports, use the **show debug interface fc?** command.

```
show debug interface fc? [hosts | stats]
```

Table 79: Syntax Description

fc?	Display debug information for the specified internal FC interface switch ports. When you type the show debug interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
hosts	Keyword used to display FC hosts information.
stats	Keywords used to display statistics and configuration information.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
2.5.1	This command was introduced for the HP SR2122.
3.2.1	This command was introduced for the HP SR2122-2.

The **show debug interface fc?** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following example displays debug information for the internal FC interface switch port *fc0*:

```
[HP SR2122-2_PR]# show debug interface fc0
```

```
[HP SR2122-2_PR]# show debug interface fc0
```

Operational Data

Interface	Stat	IP/Netmask	MAC	Options
fc0	up			type Fibre
Channel				OperState
enabled				PortID 010000
				WWN
200000059ba69821				LinkSpeed
2Gb/s				LinkState
Active				SyncState
SyncAcquired				LoginStatus
LoggedIn				Loopback
Status Not Running				MaxCredit 12
				DonatedToPort
None				RunningType
f-port				PendingType
f-port				InBandMgmt
enabled				SFPTType
NotApplicable				SFPVendor N/A
				SFPVendorID
N/A				SFPPartNumber
N/A				SFPRev N/A

Configuration Data


```

Time Port-      Al-      Ext      Fan-      Link  Loopback Mfs-
Interface Status  fairness credit enable  speed type      bundle
out  type  mode
-----
fc0      enabled  disabled 0          enabled  2Gb/s Unknown  enabled
10      f-port

```

Related Commands

Command	Description
<code>debug interface fc?</code>	Enable IP packet tracing for the specified Gigabit Ethernet interface.

show devices

To display a list of devices found or find new devices on the SR 2122 Fibre Channel network, use the `show devices` command.

Syntax

```
show devices rediscover
```

Table 80: Syntax Description

<i>rediscover</i>	Begin a new discovery process on the Fibre Channel network and display a list of all discovered devices. Notice rediscovery is done on both the fc1 and fc2 ports.
-------------------	--

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display information about all devices discovered on the storage router Fibre Channel interface. This information can be used when assigning targets to SCSI routing instances. The storage device information includes the lunid, WWPN, portid, LUN number, vendor, product name, and serial number.

Use the **rediscover** keyword to clear the existing list of devices and begin a new discovery process on the SR 2122 Fibre Channel network. Issue the `show devices` command again to display all discovered devices.

Note: The portid (ex. 0x102e2) contains both the port and domain id values.

Examples

The following is example output from the `show devices rediscover` command, followed by the `show devices` command:

show devices rediscover

Fibre channel discovery kicked off!

show devices

Private/Public Loop Devices detected

Interface	WWPN	Loopid	Device	Type	Lun	Lunid	Type
Lunid							

fc2	2200002037a70d07	2	DASD	0	IEEE	Extended	
-----	------------------	---	------	---	------	----------	--

20000002037a70d07

fc2	2200002037bb0b17	1	DASD	0	IEEE	Extended	
-----	------------------	---	------	---	------	----------	--

20000002037bb0b17

Fabric Attached Devices detected

Interface	WWPN	Portid	Device	Type	Lun	Lunid	Type
Lunid							

fc1	2200002037a70d06	0x1005e4	DASD	0	IEEE	Extended	
-----	------------------	----------	------	---	------	----------	--

20000002037a70d06

Lun Description Table

Interface	WWPN	Lun	Capacity	Vendor	Product	Serial
fc2	2200002037a70d07	0	17GB	SEAGATE	ST318451FC	

3CC028P500007101EPMF

fc2	2200002037bb0b17	0	17GB	SEAGATE	ST318451FC	
-----	------------------	---	------	---------	------------	--

3CC0690300007116DSTA

fc1	2200002037a70d06	0	17GB	SEAGATE	ST318451FC	
-----	------------------	---	------	---------	------------	--

3CC028P500007108EPMF

Table 81 describes the significant fields shown in the display.

Table 81: show devices Field Descriptions

Field	Description
Lunid	LUN identifier to be used when lun mapping with lun identifier. An attempt is made to give all luns a unique identifier
Lunid Type	The format of LUN identifier displayed, e.g. IEEE Extended, IEEE Registered Extended, MD5, and so on
WWPN	World-wide port name (WWPN) address
Loopid	The arbitrated loop ID
Portid	The fabric network port ID

Table 81: show devices Field Descriptions (Continued)

Field	Description
Device Type	The type of storage medium, for example DASD or sequential
Lun	The physical LUN associated with the device.
Capacity	The capacity of the lun to the nearest GB, MB, or KBs determined from a Read Capacity command
Vendor	The vendor of the storage device (from Inquiry data)
Product	The vendor product identifier of the storage device (from Inquiry data)
Serial	The serial number of the storage device (from Inquiry data)

show hosts

To display Fibre Channel hosts, use the `show hosts` command.

Syntax

```
show hosts
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The Fibre Channel host information is useful to debug situations where the attached devices can not be seen because a target was added with a WWPN or WWNN that does not match any of the known initiators. The host information is stored in the port database with the role set to initiator.

Examples

The following example sets the Fibre Channel switch interface to diagnostic mode.

```
show hosts
Fibre Channel Host Information
Interface  Host wwpn          wwnn                  portId
-----
fc2        200000023d070ce1    200000065d070cf1    0x203de
```

Table 82: show hosts Field Description

Parameter	Description
interface	Name of a Fibre Channel interface (fc?)
Host wwpn	The world-wide port number (WWPN) address
wwnn	The world-wide node name (WWNN) address
portid	The port ID

show interface

To display operational characteristics and statistics for interfaces configured for the storage router, use the `show interface` command. Statistics are cumulative since the last time the system was started.

Syntax

```
show interface brief
show interface [ifname / all] [stats]
show interface ifname iscsiLogins
```

Table 83: Syntax Description

<code>brief</code>	Show basic operational characteristics for all interfaces, including status, IP address, and selected options (Optional)
<code>ifname</code>	Show basic operational characteristics and configuration data for the specified interface (Optional)
<code>all</code>	Keyword used to show all operational and configuration data for all interfaces (Optional)
<code>stat</code>	Show operational statistics, such as number of input and output packets, for the specified interface (Optional)
<code>iscsiLogins</code>	Show iSCSI host logins for the specified interface. This keyword is only valid when the storage router is deployed for transparent SCSI routing.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

- Use the `show interface` command with no parameters to display the basic operational characteristics for all interfaces defined for the SR 2122.
- Use the `show interface if-name stats` command to display operational statistics related to the specified interface, including packets received and transmitted, collisions, octets, multicast packets, dropped and unsupported protocol, exception status IOCBs (such as LIP reset aborts, port unavailable or logged out, DMA errors, port configuration changed, command timeout, data overrun, write or read underrun, queue full), Fibre Channel errors, and other general events.
- Use the `show interface brief` command to display basic operational characteristics for each of the storage router interfaces. This display includes status information for the interface (up or down), and selected operational options, such as type of interface, MTU size, and speed.

Examples

The following is example output from the `show interface stats` command:

show interface fc1 stats

```
loop: LOOP READY
connection: F Port
Data Rate: 1 Gb/s
port id: 0x100100
ALPA: 0x0
firmware: READY
```

SCSI stats:

```
20 status IOCB
0 type 1 IOCB
4 marker IOCB
0 unhandled IOCB
```

```
WWPN: 28 00 00 02 3d 07 0c e0
```

SCSI Initiator stats:

```
20 SCSI Command status IOCBs
Breakdown of Exception status IOCBs:
0000000000 LIP Reset Aborts
0000000000 DMA Errors
0000000000 Port Unavailable
0000000000 Port Logged Out
0000000000 Port Configuration Changed
0000000000 Command Timeout
0000000000 Data Overrun
0000000000 Write Data Underrun - (No Data)
0000000000 Read Data Underrun - (No Data)
0000000000 Queue Full
0 type 1 IOCBs
4 marker IOCBs
0 unhandled IOCBs

0 SCSI Commands terminated by Firmware Restart
0 SCSI Commands terminated by Loop Down
0 SCSI Commands terminated by Invalid Target
```

```
bytes read      bytes written
0000000000000000 0000000000000000 (hex)
```



```

0000000014 Get All Next Requests Sent
0000000014 Get All Next Accepts Received
0000000000 Get All Next Rejects Received

```

Lun discovery information:

```

portid=0x102e1 WWPN = 21 00 00 20 37 c5 9d 28 :
1 luns reported, ALL luns discovered.
portid=0x102e2 WWPN = 21 00 00 20 37 19 12 cc :
1 luns reported, ALL luns discovered.
portid=0x102e4 WWPN = 21 00 00 20 37 c5 2f 42 :
1 luns reported, ALL luns discovered.
portid=0x102e8 WWPN = 21 00 00 20 37 c5 88 d2 :
1 luns reported, ALL luns discovered.

```

SCSI Target stats:

```

-----
0 Receive Failures

```

WWPN: 28 00 00 02 3d 07 0c e0

FC stats:

```

-----
                ERRORS                                GENERAL
0000000000 link fail          0000000000 Loop Initializations (LIP F7)
0000000001 sync loss          0000000000 Loop Failures (LIP F8)
0000000001 sig loss           0000000000 Loop Resets (LIP FF)
0000000000 CRC error          0000000001 Loop Up Events
0000000000 unhand async       0000000000 Loop Down Events
-----                    0000000001 Port Data Base Changed Events
0000000002 loop total         0000000000 Fabric Change Notifications

```

The following is an example output from the `show interface brief` command:

```
show interface brief
Interface  Stat  IP/Netmask      MAC           Options
-----
lo0        up    127.0.0.1/ff0000 0000000000 type Loopback
                                     mtusize 32768
                                     speed 0
                                     flags UP LOOPBK

RUNNING MLTCST
mgmt       up    10.1.10.205/ff00 01640f1a0 type Ethernet
                                     mtusize 1500
                                     speed 100000000
                                     flags UP BRDCST

RUNNING MLTCST
ha         up    11.1.1.205/fff00 01640f1a1 type Ethernet
                                     mtusize 1500
                                     speed 100000000
                                     flags UP BRDCST

RUNNING MLTCST
fc1        down                                     type Fibre Channel
                                     loop LOOP DOWN
                                     connection unknown
                                     port id 0x0
                                     datarate 1 Gb/s
                                     ALPA 0
                                     firmware LOSS_OF_SYNC

fc2        up                                     type Fibre Channel
                                     loop LOOP READY
                                     connection F Port
                                     port id 0x100100
                                     datarate 1 Gb/s
                                     ALPA 0
                                     firmware READY

ge1        up    10.10.10.205/ff0 02d644cd type Gigabit Ethernet
                                     mtusize 1500
                                     speed 1000000000
                                     flags UP BRDCST

RUNNING MLTCST

complete                                     signal detect
                                     duplex full
                                     auto-negotiate

                                     flow control full
                                     SFPVendor
```

```

HP-PICOLIGHT
                                SFPVendorID P200KMY
                                SFPPartNumber

PL-XPL-00-S23-40
                                SFPRev PL-00-S23-40

ge2          down  10.10.10.204/ff0  023d64cd
                                type Gigabit Ethernet
                                mtusize 1500
                                speed 1000000000
                                flags BRDCST RUNNING

MLTCST
                                signal no signal
                                duplex half
                                auto-negotiate in

progress
                                flow control none
                                SFPVendor unknown
                                SFPVendorID unknown
                                SFPPartNumber unknown
                                SFPRev unknown

```

[Table 84](#) describes the significant fields shown in the display.

Table 84: show interface Field Description

Field	Description
Interface	The interface name
Stat	The status of the interface
IP/Netmask	The IP address and network mask of the interface
MAC	The MAC address of the interface
Options	Configuration and operational information about the interface, including interface type, MTU size, speed, and activity information

show interface

Fibre Channel Server Commands

8

This section describes all the CLI commands related to the setting and monitoring of the FC server feature in the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

clear counters fc-server

To reset accumulated operational statistics for the specified FC server instance, use the `clear counters fc-server` command.

Syntax

```
clear counters fc-server {name | all} connection
```

Table 85: Syntax Description

name	The name of the FC server instance for which counters will be cleared
all	Clear counters for all FC server instances
connection	Clear operational statistics related to connections only

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

This command resets the specified operational statistics. It does not display the accumulated statistics before resetting the counters.

Examples

The following example clears the connection counters for the FC server instance *Lab1*. You might want to clear various statistics if you want to troubleshoot a connection problem.

```
clear counters scsirouter Lab1 connection
```

delete fc-server

To delete the named elements from the FC server instance, use the `delete fc-server` command. Deletions do not change the persistent storage router configuration until the relevant configuration information has been saved using the appropriate `save` command with the **bootconfig** keyword.

Syntax

```
delete fc-server {all | name} server {name | all}
delete fc-server {all | name} serverif ge?
delete fc-server {all | name} serverif ge? vlan vid
```

Table 86: Syntax Description

<i>all</i>	Delete the specified elements from all FC server instances
<i>name (?)</i>	The name of the FC server instance
<i>serverif ge?</i>	Delete the Gigabit Ethernet interface for the named FC server instance (Optional)
<i>vlan vid</i>	Delete the specified VLAN from the named FC server Gigabit Ethernet interface (Optional)
<i>server name</i>	Delete the named connection to a SCSI routing instance from the configuration for the named FC server instance (Optional)
<i>server all</i>	Delete all connections to SCSI routing instances from the configuration for the named FC server instance (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

FC server instances connect to SCSI routing instances running in remote storage routers to obtain access to storage targets. The default FC server that is created during initial system configuration is called *defaultFC*. The local name (server name) of the initial connection to a SCSI routing instance running in a remote storage router (also configured during initial system configuration) is *remoteIscsi*.

Examples

The following example deletes all connections to SCSI routing instances associated with the FC server instance named *defaultFC*:

```
delete fc-server defaultFC server all
```

fc-server autoconfig

To enable automatic configuration of storage targets seen by FC hosts connected to the named FC server instance, use the `fc-server autoconfig` command.

Syntax

```
fc-server name autoconfig {yes / no}
```

Table 87: Syntax Description

<i>name</i> (?)	The name of the FC server instance
<i>yes</i>	Keyword, used to enable automatic configuration of storage targets for the named FC server instance. This is the default setting.
<i>no</i>	Keyword, Disable automatic configuration of storage targets for the named FC server instance

Defaults

Automatic configuration mode is enabled for iSCSI clients.

Command Modes

Administrator.

Usage Guidelines

The auto configuration feature allows the FC server instance to automatically connect to all associated SCSI routing instances and display a list of available storage targets to the FC hosts. Up to 31 targets can be presented to the FC hosts via the FC server instance. If there is a problem with the FC server instance, or if you want to prevent FC hosts from seeing storage targets for any reason, use the `fc-server autoconfig no` command. The associated targets will reappear when the auto configuration option is enabled.

Each storage router can have only one FC server instance using automatic configuration of storage targets.

Examples

The following example enables automatic configuration of storage targets for the FC server instance *Cfoo1*:

```
fc-server Cfoo1 autoconfig yes
```

The following example disables automatic configuration mode for the FC server instance named *Cfoo2*:

```
fc-server Cfoo2 autoconfig no
```

scsirouter client authenticate

To enable AAA authentication for the named iSCSI client, use the `scsirouter client authenticate` command.

Syntax

```
scsirouter name client authenticate {yes | no}
```

Table 88: Syntax Description

<i>name</i>	The name of the SCSI routing services instance
<i>client</i>	Keyword used to indicate that the SCSI routing services instance is functioning as an iSCSI client

Table 88: Syntax Description (Continued)

<code>authenticate</code>	Keyword indicating AAA authentication
<code>yes</code>	Keyword used to enable AAA authentication for the named iSCSI client
<code>no</code>	Keyword used to disable AAA authentication for the named iSCSI client

Defaults

AAA authentication is disabled.

Command Modes

Administrator.

Usage Guidelines

AAA authentication for servers using the named iSCSI client will be performed based on the AAA authentication method for servers requesting access to storage devices via SCSI routing services enabled and configured on the storage router. Use the `aaa new-model` command to enable AAA authentication; use the `aaa authentication iscsi` command to configure the AAA authentication methods.

Examples

The following example enables AAA authentication for the iSCSI client named *Cfoo1*:

```
scsirouter Cfoo1 client authenticate yes
```

Table 89: Command History

Command	Description
<code>aaa authentication scsi</code>	Enables an AAA authentication method for servers requesting access to storage devices via SCSI routing services
<code>aaa new-model</code>	Enables the AAA access control model
<code>copy aaa</code>	Copies AAA configuration information
<code>restore aaa</code>	Restores AAA configuration information from the named configuration file

Table 89: Command History (Continued)

Command	Description
<code>scsirouter</code>	Creates the named SCSI routing services entity
<code>scsirouter client autoconfig</code>	Enables automatic configuration mode for the named iSCSI client.
<code>scsirouter client password</code>	
<code>scsirouter client server</code>	Associates the IP address of other storage routers that provide access to storage devices to the iSCSI client.
<code>scsirouter client username</code>	
<code>show aaa</code>	Displays current AAA configuration information
<code>show session</code>	Displays configuration and operational information about the named iSCSI client

fc-server description

To add user-defined identification information to the named FC server instance, use the `fc-server description` command.

Syntax

```
fc-server name description "text"
```

Table 90: Syntax Description

<i>name</i>	The name of this FC server instance.
<i>description</i> <i>"text"</i>	User-defined identification information associated with this FC server instance. If the string contains spaces, enclose it in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `fc-server description` command lets you add a new description or change an existing description. Descriptions are site-specific.

Examples

The following example adds the description “Access to WebServer4 WebServer5” to the FC server *fool*:

```
fc-server fool description "Access to Tom's Webservers[4-5]"
```

fc-server enable

To start the named FC server instance, use the `fc-server enable` command. To stop the named FC server instance, use the `no` form of this command.

Syntax

```
fc-server {name / all} enable  
no fc-server {name / all} enable
```

Table 91: Syntax Description

<i>name</i>	The name of the FC server instance to be started
<i>all</i>	Keyword, indicating all instances or extensions on this storage router

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

To restart a stopped FC server instance, use the `fc-server enable` command. Use the **all** keyword to start all instances on the storage router. All instances previously stopped on this storage router will be started. FC server instances are automatically started by the storage router when the Fibre Channel interface is added.

Examples

The following example starts the FC server instance named *foo1*. This instance must have been previously stopped:

```
fc-server foo1 enable
```

fc-server server

To identify the Gigabit Ethernet IP addresses of the SCSI routing instances (running in remote SR 2122 Storage Routers) that provide access to storage resources for the named FC server instance, use the `fc-server server` command.

Syntax

```
fc-server name server name A.B.C.D [username password]
```

Table 92: Syntax Description

<i>name (?)</i>	The name of the FC server instance
<i>server name</i>	A meaningful name to associate with the IP address of the SCSI routing instance providing the FC server instance access to storage devices
<i>A.B.C.D</i>	The IP address of the Gigabit Ethernet interface associated with the SCSI routing instance in the remote SR 2122 Storage Router
<i>username</i>	The username associated with the remote iSCSI server
<i>password</i>	The password for this username

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use this command to identify a SCSI routing instance in a remote SR2122 Storage Router that is available to the FC server instance via its Gigabit Ethernet interface. You can associate multiple SCSI routing instances (running in one or more remote storage routers) with a single FC server instance by issuing this command several times. The specified SCSI routing instance provides the FC server instance access to storage targets. Up to 31 storage targets can be made available to the FC server instance. The **server name** keyword/variable pair allows you to associate a meaningful local name with the IP address. If the remote Storage Router has AAA enabled and needs a username/password, then the username/password entered will be used during the authentication phase of the iScsi login. If the remote Storage Router does not have AAA enabled, then a username/password is not required.

Examples

The following example associates the name *labserver1* to the SCSI routing instance with the Gigabit Ethernet IP address *10.1.10.145* for the FC server instance named *Cfoo1*. All storage targets available through the Fibre Channel interface of the SCSI routing instance at *10.1.10.145* are made available to the FC server instance named *Cfoo1*. The second example is for the same server, but includes the username/password.

```
fc-server Cfoo1 server labserver1 10.1.10.145
fc-server Cfoo1 server labserver1 10.1.10.145 lab001 m76G41
```

fc-server serverif

To assign a Gigabit Ethernet interface and IP address to the named FC server instance, use the `fc-server serverif` command. The interface allows access to storage devices through a SCSI routing instance running on a remote storage router.

Syntax

```
fc-server name serverif ge? <A.B.C.D/bits | A.B.C.D/1.2.3.4>  
fc-server name serverif ge? vlan <vid> <A.B.C.D/bits |  
A.B.C.D/1.2.3.4>
```

Table 93: Syntax Description

<i>name (?)</i>	The name of the FC server instance to which you are adding the Gigabit Ethernet interface
<i>serverif ge?</i>	The name of the interface. When you type the <code>fc-server serverif</code> command, followed by <code>?</code> , the CLI lists the interfaces available. You cannot specify a nonexistent interface.
<i>A.B.C.D/ bits</i>	The IP address of the named interface. If the keyword vlan is used, the IP address is on the specified VLAN. A.B.C.D is the dotted quad notation of the IP address. The <code>/bits</code> specifies the subnet mask in CIDR style.
<i>A.B.C.D/ 1.2.3.4</i>	The IP address of the named interface. If the keyword vlan is used, the IP address is on the specified VLAN. A.B.C.D is the dotted quad notation of the IP address. 1.2.3.4 is the dotted quad notation of the subnet mask.
<i>vlan vid</i>	The keyword and the virtual LAN identifier

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Each FC server instance requires three active elements:

- The *server* element associates the FC server instance with a SCSI routing instance in a remote storage router. The specified SCSI routing instance provides the FC server instance access to storage.
- The *serverif* element assigns the Gigabit Ethernet interface and IP address used to communicate with storage devices via a SCSI routing instance in a remote storage router.
- The `fc-server serverif vlan` command is used to associate a VLAN with a FC server instance. All traffic using the specified Gigabit Ethernet interface will be considered as part of the VLAN.

When the FC server instance is started, a logical interface is created with a name that incorporates the VID and the physical interface, such as *ge2VLAN100*. This logical interface can be displayed via the `show interface` command and can be used when adding static routes to the system.

Examples

The following command adds the Gigabit Ethernet interface *ge2*, with the IP address *10.1.10.20/24*, to the FC server instance named *foo1*:

```
fc-server foo1 serverif ge2 10.1.0.20/24
```

The following command adds the Gigabit Ethernet interface *ge2* as VLAN ID 45, with IP address *11.1.30.20/24*, to the FC server instance *foo2*:

```
fc-server foo2 serverif ge2 vlan 45 11.1.30.20/24
```

show debug fc-server

To display a variety of Fibre Channel debug information or to perform specific troubleshooting activities, use the `show debug fc-server` command.

Syntax

```
show debug fc-server {name | all} stcstatus
show debug fc-server {name | all} tbestatus
show debug fc-server {name | all} tbetrace
```


Table 94: Syntax Description

all	Displays information for all FC server instances
name	Displays the name of the FC server instance
stcstatus	Displays trace status data for the specified FC server instance
tbestatus	Displays the status of the trace activity for the specified FC server instance
tbetrace	Displays the trace information for the specified FC server instance

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Some `show debug fc-server` commands may perform actions that drop existing connections or otherwise impact normal storage router performance. The `show debug fc-server` command is designed for debugging purposes; it should only be used under the guidance of a HP Technical Support professional.

Examples

The following example displays TBE status data for the FC server instance named *foo*:

```
show debug fc-server foo tbestatus
```

show fc-server

To display configuration information and operational statistics related to an FC server instance, use the `show fc-server` command.

Syntax

```
show fc-server
show fc-server name all
show fc-server {name | all} [from {bootconfig | runningconfig |
filename}]
show fc-server {name | all} brief
show fc-server {name | all} {servers | targets}
show fc-server {name | all} connection [stats | tcp]
show fc-server {name | all} serverif [from {bootconfig
/runningconfig | filename}]
show fc-server {name | all} hosts
show fc-server {name | all} stats
show fc-server {name | all} targets
```

Table 95: Syntax Description

<i>name</i>	Displays the name of the FC server instance
<i>name all</i>	Displays all configuration information about the specified FC server instance
<i>all</i>	Displays the requested information about all FC server instances
<i>from bootconfig</i>	Displays the requested FC server instance configuration information from the persistent saved configuration (Optional)
<i>from running</i>	Displays the requested FC server instance configuration information from the currently running configuration (Optional)
<i>from filename</i>	Displays the name of the saved configuration file containing the specified FC server instance information. This file must exist in the savedconfig directory. (Optional)
<i>brief</i>	Displays brief configuration information (Optional)
<i>connection</i>	Displays connection information for the named FC server instance (Optional)
<i>hosts</i>	Displays status and other operational data for FC hosts currently connected to the named FC server instance (Optional)

Table 95: Syntax Description (Continued)

<code>serverif</code>	Displays configuration information for the Gigabit Ethernet interface associated with the named FC server instance (Optional)
<code>servers</code>	Displays information about the SCSI routing instances providing the FC server instance access to storage resources (Optional)
<code>stats</code>	Displays accumulated operational information about the FC server instance. This display shows statistics accumulated since the named FC server instance became active or statistics were last cleared, whichever is more recent. (Optional)
<code>targets</code>	Displays operational information about storage targets available to the named FC server instance (Optional)
<code>tcp</code>	Displays current and maximum TCP window size for each connected SCSI routing instance (Optional)

Defaults

The `show fc-server` command with no parameters displays the name of all FC server instances running on the storage router. When **no from** parameters are specified, the information displayed is from the currently running configuration.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the optional keywords **targets** and **serverif** to restrict the display to FC server instance configuration information related to those objects. For example:

- The command `show fc-server name targets` displays current configuration information for all storage targets available to the named instance, including the total number of discovered targets, and information about targets associated with each SCSI routing instance to which the FC server instance is connected.
- The command `show fc-server all serverif` displays current configuration information for the Gigabit Ethernet interfaces associated with all FC server instances in the storage router.

Use the **connection** or **hosts** keywords to display specific operational data for the named FC server instance.

- The command `show fc-server name hosts` displays status and operational statistics for currently connected FC hosts.
- The command `show fc-server name stats` displays accumulated operational information about all FC hosts that have been connected since the named instance became active. Operational statistics include login and active counts.
- The `show fc-server all stats` command is useful for determining quick operational status of all FC server instances running in the storage router.
- Use the `show fc-server all` command to display configuration information for all FC-server instances, including descriptions, interface, and the local name and Gigabit Ethernet IP address for all associated SCSI routing instance.

Examples

The following is an example output from the `show fc-server` command:

```
show fc-server
all
defaultFC
```

The following is example output from the `show fc-server stats` command:

```
show fc-server defaultFC stats
router      status  started          iSCSI ver (Min/Max) logins
active
defaultFC   ACTIVE   Jan 09 21:54:11  2/2                10      10
```

[Table 96](#) shows the FC server stats field descriptions:

Table 96: show fc-server Field Description

Field	Description
router	The name of the FC server instance
status	Indicates if the instance is active or inactive
started	The date and time the FC server instance was last started
iSCSI ver (min/max)	The iSCSI draft version information (minimum and maximum version that is used by the FC server instance)
logins	The total number of logins attempted
active	The total number of active connections

show fc-server

HA Commands

9

This section describes all the CLI commands related to the high availability (HA) feature in the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

clear scsirouter failover

To clear the designation of primary or secondary nodes from the HA failover list for the specified SCSI routing instance, use the `clear scsirouter failover` command.

Syntax

```
clear scsirouter name failover primary
clear scsirouter name failover secondary
```

Table 97: Syntax Description

name (?)	The name of the SCSI routing instance
primary	Keyword, delete the current primary storage router from the HA failover list
secondary	Keyword, delete the secondary storage router from the HA failover list

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `clear scsirouter failover` command to remove the primary or secondary priority designation of a node on the HA failover list for the specified SCSI routing instance. SCSI routers that fail with no failover primary or secondary specified will fail over to the first node on the failover list. (The first node on the failover list will be a node with an eligibility to run the instance equal to or greater than the other nodes in the cluster.)

Use the `scsirouter failover` command to prioritize a node on the HA failover list. (Placement of a node on the failover list is determined first by eligibility to run the instance and then by any priority assigned to that node.)

This command saves the SCSI routing instance configuration information and updates all nodes in the cluster.

Examples

The following example removes the secondary priority designation of the node on the HA failover list for SCSI routing instance *foo*:

```
clear scsirouter foo secondary
```

failover scsirouter

To cause the named SCSI routing instance to stop running on the storage router and start running on another storage router in the cluster, use the `failover scsirouter` command.

Note: If no eligible storage router is found, the SCSI routing instance will start running again on the same storage router. If the storage router is configured as a standalone system, failover is not allowed.

Syntax

```
failover scsirouter {name / all}
failover scsirouter name {pri / sec}
failover scsirouter {name / all} to sysname
```

Table 98: Syntax Description

name(?)	The name of the SCSI routing instance to be failed-over
all	Failover all instances currently running on this storage router
pri	Force failover to the designated primary storage router in the failover list
sec	Force failover to the designated secondary storage router in the failover list
to sysname (?)	Perform the failover to the specified storage router. This storage router must be active in the cluster.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the **all** keyword to fail over all SCSI routing instances currently running on this storage router. Each storage router can run a maximum of 12 SCSI routing instances; there is a maximum of 12 SCSI routing instances per cluster.

Examples

The following example causes the SCSI routing instance named *foo* to failover to another storage router in the cluster:

```
failover scsirouter foo
```

interface ha

To set various operational parameters associated with the high availability (HA) interface, such as the speed and duplex mode, use the **interface ha** command.

```
interface ha autonegotiation
interface ha no autonegotiation [speed {10 | 100}] [duplex
{full | half}]
```

Table 99: Syntax Description

autonegotiation	Auto negotiation will always be used on this interface. Operational characteristics will automatically be negotiated with the partner.
speed 10	(Optional) The interface speed is fixed at 10 Mbps. Auto negotiation is not used.
speed 100	(Optional) The interface speed is fixed at 100 Mbps. Auto negotiation is not used. If speed is not specified, the default is 100 Mbps.
duplex full	(Optional) The duplex setting is fixed at full. Auto negotiation is not used. If the duplex setting is not specified, the default is full duplex.
duplex half	(Optional) The duplex setting is fixed at half. Auto negotiation is not used.

Defaults

Auto negotiation is enabled.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to manually set a specific interface speed and duplex setting, if the partner is unable to auto negotiate these settings.

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover to provide consistent performance characteristics. Use the **show interface ha** command to display current operating characteristics for the HA interface.

Examples

The following example disables auto negotiation, and sets the interface speed to 10 Mbps, duplex full:

```
[HP SR2122-2-2] interface ha no autonegotiation speed 10 duplex full
```

Related Commands

Command	Description
<code>interface ha ip-address</code>	Specify the HA interface IP address and subnet mask.
<code>show interface</code>	Display operational and configuration information for the specified interface or all interfaces.

scsirouter failover

To prioritize a list of nodes to be used for failover purposes, use the `scsirouter failover` command.

Syntax

```
scsirouter name failover primary sysname
scsirouter name failover secondary sysname
```

Table 100: Syntax Description

<code>name (?)</code>	The name of the SCSI routing instance
<code>primary</code>	The name of the node in the cluster. In case of failure, the specified SCSI routing instance will be failed over to this node.
<code>secondary</code>	The name of the node in the cluster. If the primary storage router in the list cannot run the SCSI routing instance, it will be failed over to this node. (Optional)
<code>sysname (?)</code>	The name of the storage router in the cluster

Defaults

None. By default, the HA failover list is ordered randomly.

Command Modes

Administrator.

Usage Guidelines

Use the `scsirouter failover` command to prioritize nodes that will be used during the failover process. Assuming that the nodes designated by this command as primary and or secondary have an eligibility to run the instance equal to or greater than the other nodes in the cluster, the order of failover will be primary node and then secondary node.

If there is no designated primary or secondary node on the HA failover list when the SCSI routing instance fails over, the cluster attempts to run the instance on the first available node on the failover list. The first node on the failover list will always be a node that is equal to or greater than the eligibility of the other nodes in the cluster.

Use the `show scsirouter name failover` command to get a list of failover nodes by priority; the first item is highest priority and the last item is lowest priority. This command lists the configured failover preferences (if any) and then shows the actual failover list, which always includes all the active nodes in the cluster. The only effect of the user-configured primary and secondary is to modify the initial order of this list.

Use the `clear scsirouter failover` command to remove the designated primary or secondary node on the HA failover list.

Examples

The following example reorders the priority of the HA failover list for the SCSI routing instance named *foo*. The primary storage router in the HA failover list is HP SR2122-2A and the secondary is HP SR2122-2B. This priority on the failover list can change if the eligibility to run the specified `scsirouter` instance is downgraded due to the loss of an interface or configured devices.

```
scsirouter foo failover primary HP SR2122-2A
scsirouter foo failover secondary HP SR2122-2B
```

scsirouter password

To set the password that will be used to compute the response to an authentication request from an iSCSI initiator, use the `scsirouter password` command.

Syntax

```
scsirouter {name password string}
```

Table 101: Syntax Description

name	The name of the SCSI routing services instance
password	The keyword used to identify the password associated with this instance
string	The password string

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `scsirouter password` command to set the password used to compute the response to an authentication request from an iSCSI initiator. If no password is configured, any authentication request sent by an iSCSI initiator will result in an login error by the `scsirouter`.

Examples

The following example sets the password for the SCSI routing instance named *foo* to *testing*:

```
[HP SR2122-2]# scsirouter foo password testing
```

The following example deletes the password for the SCSI routing instance named *foo*.

```
[HP SR2122-2]# scsirouter foo password none
```

scsirouter primary

To assign the storage router as the preferred storage router for the named SCSI routing instance, use the `scsirouter primary` command. To remove the current preferred storage router setting, use the `scsirouter name primary none` command.

Syntax

```
scsirouter name primary sysname  
scsirouter name primary none
```

Table 102: Syntax Description

name (?)	The name of this SCSI routing instance
none	No preferred storage router
sysname	The system name of the preferred storage router

Defaults

The primary attribute defaults to **none** (no preferred storage router).

Command Modes

Administrator.

Usage Guidelines

At any given time, a SCSI routing instance can run on only one storage router in a cluster. If an iSCSI routing instance has the primary attribute set, the specified node (upon system restart) will take over running that instance. Use the `scsirouter primary` command if you *always* want the specified SCSI routing instance to run on a specific node in a cluster when that node has all the resources configured for that `scsirouter`. Configuring a node as primary for a `scsirouter` instance while active on another node in the cluster will cause the active `scsirouter` to move to the newly configured primary node.

If the primary attribute is not set (the default condition), the SCSI routing instance continues running on the storage router where it was started until:

- It is explicitly stopped (via a `no scsirouter enable` command)
- It automatically fails over to another storage router in the cluster because an interface is unavailable
- A system failure occurs
- An explicit `failover scsirouter` command is issued

Examples

The following command designates the node at IP address `server1` as the node on which the SCSI routing instance named `foo1` will always run, providing it has access to all resources configured for router instance `foo1`.

```
scsirouter foo1 primary server1
```

The following example resets the primary attribute for the SCSI routing instance named `foo2`. If the routing instance is active on the node that was specified as the primary, the instance named `foo2` will continue to run on this node until:

- It is explicitly stopped
- It automatically fails over
- An explicit `failover scsirouter` command is issued

```
scsirouter foo2 primary none
```


show cluster

To display operational information related to the storage router cluster, use the `show cluster` command.

Syntax

```
show cluster
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

The `show cluster` command displays the following fields:

Table 103: show cluster Field Descriptions

Field Name	Data Format	Description
Cluster Name	string	The name of storage router cluster
Cluster Changes	decimal	The number of changes to cluster configuration since last restart
Last Change	date	The date and time of the last cluster configuration change
IP Multicast Address	string	The IP address used for multicast communications. IANA has assigned the multicast IP address 224.0.0.101 to the HP SR2122-2 Storage Router.
Local Node	string	The name of the storage router
HA Configuration	string	Indicates the configuration of HA in the storage router. Valid configurations are standalone.

Table 103: show cluster Field Descriptions (Continued)

Field Name	Data Format	Description
HA	string	Indicates the state of the HA application in the storage router. Valid states are "up" or "down". If the storage router HA configuration is standalone, the HA state should be "down."
MGMT Port	string	Indicates the state of the storage router's physical management port. Valid states are "up" or "down."
HA Port	string	Indicates the state of the storage router's physical HA port. Valid states are "up" or "down."
Sent heartbeats	decimal	The number of heartbeats transmitted on the high availability (HA) network
Recvd heartbeats	decimal	The number of heartbeats received on the HA network
Cluster Node List	string	The list of storage routers in the cluster
System name	string	The system name
MGMT IP	IP address	The management interface IP addresses of this storage router and the other cluster member
HA IP	IP address	The HA interface IP address of this storage router and the other cluster member
Last Heard From	date	The date the cluster member was last heard from
Application Name	string	Name of the active SCSI routing instance. For example, scsirouter/scsi1 or scsirouter/mySCSI
Master on	system name	The name of the storage router currently running this SCSI routing instance
State	string	The state of the SCSI routing instance
Last Config Update	date	The date and time of the last configuration change to this SCSI routing instance
Access List and VLAN Management	string	The name of the storage router in the cluster that currently handles access list and VLAN management

Examples

The following example displays cluster information about a storage router that belongs to a cluster:

```
show cluster
Cluster Name: douglas
Cluster Changes: 2
Last Change: Thu Feb 28 14:58:27 GMT 2002
IP Multicast Address: 224.0.0.101

Local Node: stimpy
HA Configuration: STANDALONE
HA: down MGMT Port:up HA Port:down
Sent 0 heartbeats
Rcvd 0 heartbeats

Cluster Node List:
System Name MGMT IP HALast Heard From IP (null)
stimpy 10.82.1.40 10.1.0.101 Self

Application List:
Application Name Master on State Last Config Update
scsirouter/d      stimpy   Master   not available
scsirouter/test   stimpy   Master   not available
scsirouter/test3  stimpy   Master   not available
scsirouter/test4  stimpy   Master   not available
scsirouter/test5  stimpy   Master   not available
scsirouter/test6  stimpy   Master   not available
scsirouter/test7  stimpy   Master   not available
scsirouter/test8  stimpy   Master   not available
scsirouter/casaba stimpy   Master   not available
scsirouter/hoover stimpy   Master   not available

Access List and Vlan Management is on stimpy
```

show ha

To display HA configuration and status information and HA statistics for the storage router or selected applications and SCSI routing instances running in the HA environment, use the `show ha` command.

Syntax

```
show ha all
show ha app {all / list / nn} stats
show ha app nn failover list
show ha node stats
```

Table 104: Syntax Description

all	Displays brief HA status and configuration information (Optional)
app all stats	Shows HA statistics for all applications (Optional)
app list stats	Displays a list of HA applications and brief HA statistics. This list includes application numbers. (Optional)
app nn stats	Displays keywords used to display HA statistics for the specified application number (Optional)
app nn failover list	Shows HA failover list for the specified SCSI routing instance (Optional)
node stats	Displays keyword used to generate a display of HA statistics for the storage router node (Optional)

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to determine if there are communications problems within the storage router cluster. The `show ha all` command displays the state of the management and HA interfaces.

To display statistics about all applications, issue this command:

```
show ha app all stats
```

To display a list of SCSI routing instances and other HA applications with their creation dates and last failover times, issue this command:

```
show ha app list stats
```

Examples

The following is an example output from the `show ha` command using the **app list** keywords to display a list of applications and SCSI routing instances:

```
show ha app list stats
-----HA APPLICATION
LIST-----

Type = cluster Created = Tue Jul 10 17:08:02 CDT 2001
(Number 1) cluster/myCluster
Created = Tue Jul 10 17:08:03 CDT 2001
Activated = Tue Jul 10 17:08:03 CDT 2001
Last Failover = no failover yet

Type = scsirouter Created = Tue Jul 10 17:08:02 CDT 2001
(Number 0) scsirouter/myScsi1
Created = Wed Jul 11 16:36:02 CDT 2001
Activated = Wed Jul 11 16:36:07 CDT 2001
Last Failover = no failover yet
(Number 1) scsirouter/myScsi1
Created = Wed Jul 11 18:20:14 CDT 2001
Activated = Thu Jul 12 07:45:01 CDT 2001
Last Failover = Thu Jul 12 11:15:33 CDT 2001
-----
-----
```

Table 105 describes the significant fields shown in the display.

Table 105: show ha Field Descriptions

Field	Description
Type	The type of HA application or service
Created	The date and time the application or service type was created
Number	The HA application or service number. This number is used in the <code>show ha</code> command with the app keyword to display information about that specific application or service.
Created	The date and time the specific application or service was created
Activated	The date and time the specific application or service became active
Last Failover	The date and time the specific application or service last failed over

The following is an example output from the `show ha` command, using the app **nn** keyword and parameter to display operational statistics about the SCSI instance named *myScsi1*:

```
show ha app 0 stats
----- HA APPLICATION Number
0-----
Application Name = scsirouter/myScsi1
Type = scsirouter Master Specifics: DataBase:
AppId = 072c1560 Node Id = 3d000820 ID = 8dcdb379
State = Master Preferred Slave = No Status = Up to Date

Permanent Master = No Last Update =
Fri Jul 13 00:14:59 CDT 2001

HA Message Transmission Summary:
Total = 00000005 Broadcasts = 00000002 Unicasts = 00000003
HA Message Reception Summary:
Total = 00000004

-----Message Breakdown-----
Message Types Received      Message Types Transmitted
Master Requests = 00000002   Master Requests = 00000001
Master Acks = 00000001      Master Acks = 00000002
Elections = 00000001        Elections = 00000001
Refusals = 00000000         Refusals = 00000000
Conflicts = 00000000        Conflicts = 00000000
Resolves = 00000000         Resolves = 00000000
Quits = 00000000           Quits = 00000000
Resignations = 00000000     Resignations = 00000001
Doas = 00000000            Doas = 00000000
```

[Table 106](#) describes the significant fields shown in the display.

Table 106: show ha app Field Description

Field	Description
Application Name	The complete name of the HA application. The syntax is application-type/application name.
Type	The HA application type
Appld	The HA application identification number
State	The state of the HA application
Master Specifics: Node Id	The ID of the node that is currently running the HA application
Preferred Slave	Indicates if the storage router is the first storage router on the failover list for this HA application

Table 106: show ha app Field Description (Continued)

Field	Description
Permanent Master	Indicates if the storage router is defined as the primary for this HA application
Database: ID	Unique MD5 hash value passed in HA heartbeat, if changed indicates the configuration has been modified
Status	Indicates configuration is current if "up to Date" otherwise "Update pending" indicates the configuration has been modified
Last Update	The date and time of the last update to this HA application
HA Message Transmission Summary	The number of HA messages that have been transmitted by this application. The Total value is the sum of the Broadcasts and the Unicasts.
HA Message Reception Summary	The total number of HA messages received by this application
Message Breakdown	<p>The number of each type of HA message that has been received and transmitted by this HA application. The following are HA message types:</p> <ul style="list-style-type: none"> ■ Master Requests ■ Master Acts ■ Elections ■ Refusals ■ Conflicts ■ Resolves ■ Quits ■ Resignations ■ Does

IP Commands

10

This section describes all the CLI commands related to the setting and monitoring of IP (Internet Protocol) related ports and functions in the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

clear counters fcip

To clear all counters associated with the specified FCIP instance, or all instances, use the **clear counters fcip** command.

```
clear counters fcip {name | all}
```

Table 107: Syntax Description

name	The name of the FCIP instance for which counters will be cleared.
all	Clear counters for all FCIP instances.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

User Guidelines

This command resets the specified operational statistics. It does not display the accumulated statistics before resetting the counters.

Clear counters before beginning a troubleshooting session, so you can quickly identify the counters that are changing.

Examples

The following example clears the operational counters for the FCIP instance named *fcip1*:

```
[HP SR2122-2]# clear counters fcip fcip1
```

The following example clears the operational counters for all FCIP instances:

```
[HP SR2122-2]# clear counters fcip all
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

clear counters interface

To clear all counters associated with the specified interface, or to clear all interfaces, use the `clear counters interface` command.

Syntax

```
clear counters interface all
clear counters interface ifname
```

Table 108: Syntax Description

<code>ifname</code> (?)	The name of the interface. Counters can be cleared for the management (mgmt), Fibre Channel (fc?) and Gigabit Ethernet (ge?) interfaces, and the HA interface (ha if available).
<code>all</code>	The keyword used to clear counters for all interfaces

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

This command resets all accumulated operational statistics for the specified interface. Operational statistics can include counters for packets received and transmitted, collisions, octets, multicast packets, and dropped and unsupported protocol, exception status IOCB (such as LI Preset aborts, port unavailable or

logged out, DMA errors, port configuration changed, command time out data overrun, write or read data under run, queue full), Fibre Channel errors, and other general events.

The normal use for clearing the counters before starting any debugging is quickly identifying which counters are changing.

Examples

The following example clears all accumulated operational statistics counters for the Fibre Channel interface *fc1*.

```
clear counters interface fc1
```

clear scsirouter primary

To remove the storage router configured as the primary for the named SCSI routing instance, use the **clear scsirouter primary** command.

```
clear scsirouter name primary
```

Table 109: Syntax Description

name	The name of the SCSI routing instance.
------	--

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced. For the HP SR2122-2, this command replaces the scsirouter primary command with the none keyword.

Usage Guidelines

At any given time, a SCSI routing instance can run on only one storage router in a cluster. If a SCSI routing instance has the **primary** attribute set, the specified storage router will take over running that instance upon system restart or whenever target and critical resources are available.

If the **primary** attribute is not set, the SCSI routing instance continues running on the node where it was started until it is explicitly stopped (via a **no scsirouter enable** command), it automatically fails over to another storage router in the cluster because targets or critical resources are unavailable, or an explicit **failover scsirouter** command is issued. This is the default behavior.

Examples

The following command removes the storage router configured as the primary for the SCSI routing instance named lab2:

```
[HP SR2122-2]# clear scsirouter lab2 primary
```

Related Commands

Command	Description
clear scsirouter failover	Remove the designated primary or secondary storage router from the HA failover list for the specified SCSI routing instance.
failover scsirouter	Identify the storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter failover	Add the storage router to the HA failover list for the specified SCSI routing instance.

debug ip rip

To enable routing information protocol (RIP) debug log message, use the **debug ip rip** command. To disable RIP debug log message, use the **no** form of this command.

```
debug ip rip
no debug ip rip
```

Syntax Description

This command has no arguments or keywords.

Defaults

RIP debug log messages are disabled.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

The **debug ip rip** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following example enables RIP, configures logging to send debug message to all virtual terminal sessions, and then enables RIP debug log messages. The **show ip rip** command is used to verify the running RIP configuration.

```
[HP SR2122-2]# ip rip enable
Dec 09 16:12:50: %IP-5-IRMRSAR: RIP Services are running
*[HP SR2122-2]# logging level debug from ip to vty
*[HP SR2122-2]# debug ip rip
Dec 31 12:52:14: %IP-7-IRRPRL00: RIP Packet received from 10.1.30.1
length 124
Dec 31 12:52:14: %IP-7-IRRPRL01: command 2 version 1
Dec 31 12:52:14: %IP-7-IRRPRL02: route af 2, dest 10.1.40.0
mask 0.0.0.0 nextHop 0.0.0.0 metric 2
Dec 31 12:52:14: %IP-7-IRRPRL02: route af 2, dest 10.1.51.0
mask 0.0.0.0 nextHop 0.0.0.0 metric 1

*[HP SR2122-2]# show ip rip
Routing Information Protocol (RIP) Information:
  Invalid Timer: 180
  Enabled Flag: true
  Debug Flag: true
  Running Flag: true
```

Related Commands

Command	Description
ip rip enable	Enable the storage router to learn dynamic routing using the routing information protocol (RIP).
show ip	Display entries from the storage router routing table, and statistics for the protocols used in the storage router network. Use the rip keyword to display RIP configuration information.

debug isns

To enable tracing of iSNS Protocol Data Units (PDUs), use the **debug isns** command. To disable the iSNS trace facility, use the **no** form of this command.

```
debug isns trace [pducnt nn] [pdusize nn] enable
no debug isns trace enable
```

Table 110: Syntax Description

trace	Keyword indicating iSNS PDU tracing will be enabled.
pducnt nn	(Optional) Specify the maximum number of PDUs to be traced. <i>nn</i> must be a value greater than zero (0), and cannot exceed 4294967295. If not specified, a circular trace buffer is used. This is the default.
pdu size nn	(Optional) Specify the maximum number of bytes to trace per PDU. The default is 1024 bytes.
enable	Keyword used to enable iSNS PDU tracing.

Defaults

iSNS PDU tracing is disabled. The default PDU size is 1024 bytes, and uses a circular trace buffer.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced.

Usage Guidelines

The **debug isns** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following example enables iSNS PDU tracing:

```
[HP SR2122-2]# debug isns trace enable
```

The following example enables iSNS PDU tracing, for a maximum of 100 PDUs. A maximum of 40 bytes will be traced per PDU.

```
[HP SR2122-2]# debug isns trace pducnt 100 pdu size 40 enable
```


Related Commands

Command	Description
<code>isns enable</code>	Enable communications and client registrations with an iSNS server.
<code>isns refresh</code>	Force a refresh of the iSNS server with device registrations.
<code>show debug isns</code>	Display iSNS PDU traced contents and statistics.
<code>show isns</code>	Display iSNS configuration information, objects, or operational statistics.

debug scsirouter iscsitrace

To enable trace facilities for debugging iSCSI connections to and from SCSI routing instances, use the **debug scsirouter iscsitrace** command. To disable iSCSI trace facilities, use the **no** form of this command.

```
debug scsirouter name iscsitrace [fromto
{A.B.C.D/bits | A.B.C.D/1.2.3.4}] [pducnt nn] [pdu size nn]
enable
no debug scsirouter name iscsitrace enable
```

Table 111: Syntax Description

name	The name of the SCSI routing instance to be debugged.
fromto A.B.C.D/bits	(Optional) Trace iSCSI Protocol Data Units (PDUs) from and to the specified host or network. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
fromto A.B.C.D/1.2.3.4	(Optional) Trace iSCSI PDUs from and to the specified host or network. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.
pducnt nn	(Optional) Specify the maximum number of PDUs to trace.
pdu size nn	(Optional) Specify the maximum trace size per PDU, in bytes.
enable	Enable iSCSI trace facilities.

Defaults

The following are the default iSCSI trace options:

- All client connections to and from the specified SCSI routing instance are traced.
- The maximum trace size per PDU is 48 bytes.
- All PDUs are traced (circular).
- The trace buffer size is 131072 bytes. This value cannot be changed.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

The **debug scsirouter iscsitrace** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Use the **show debug scsirouter** command with the **iscsitrace** keyword to display iSCSI trace information.

Examples

The following example enables iSCSI trace facilities for the SCSI routing instance named *zeus*, using the default iSCSI trace options:

```
[HP SR2122-2]# debug scsirouter zeus iscsitrace enable
```

Related Commands

Command	Description
<code>debug scsirouter</code>	Enable debugging for the named SCSI routing instance.
<code>debug scsirouter target</code>	Enable debugging for a specific SCSI routing instance target and LUN combination.
<code>show debug scsirouter</code>	Display trace buffer output.

interface ge?

To set various operational parameters associated with the Gigabit Ethernet interface, such as the size of the maximum transfer unit (MTU) or the use of VLANs, use the `interface ge?` command. To specify that auto-negotiation will never be used on this interface, use the `interface ge? no autonegotiation` command.

Syntax

```
interface ge? autonegotiation [autodetect]
interface ge? no autonegotiation
interface ge? mtusize {nn | default}
interface ge? vlan enabled
no interface ge? vlan enabled
```

Table 112: Syntax Description

<code>ge?</code>	Specifies the name of the interface for which you are setting this parameter. When you type the <code>interface ge?</code> command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
<code>autonegotiation</code>	Auto-negotiation will always be used on this interface.
<code>autonegotiation autodetect</code>	Automatically detects if auto-negotiation should be used for this interface. This is the default setting.

Table 112: Syntax Description (Continued)

<code>mtusize nn</code>	The size of the MTU, in bytes. nn is an integer between 1500 and 9000. Gigabit Ethernet interfaces support jumbo frames.
<code>mtusize default</code>	Resets the value to the factory default of 1500 bytes
<code>vlan enabled</code>	Enabled virtual LANs for this interface. This is the default.

Defaults

MTU size defaults to **1500** bytes; auto negotiation defaults to **autodetect**. For storage routers deployed for SCSI routing, the use of VLANs is enabled by default.

Command Modes

Administrator.

Usage Guidelines

All storage routers in a cluster should be configured with the same MTU size and other interface-specific parameters, allowing failover of applications to provide consistent performance characteristics.

Use the `no interface ge? vlan enable` command to quickly restrict VLAN functionality on the storage router's Gigabit Ethernet interface for troubleshooting purposes.

Examples

The following example enables virtual LANs for the storage router Gigabit Ethernet interface, *ge2*:

```
interface ge2 vlan enabled
```

interface ge? ip-address

To set an IP address and subnet mask for one of the gigabit ethernet interfaces for managing the system, use the `interface ge? ip-address` command.

Syntax

```
interface ge? ip-address {A.B.C.D/bits | A.B.C.D/1.2.3.4}
interface ge? ip-address {A.B.C.D/bits | A.B.C.D/1.2.3.4}
secondary ge?

interface ge? vlan vid ip-address {A.B.C.D/bits |
A.B.C.D/1.2.3.4}
interface ge? vlan vid ip-address {A.B.C.D/bits |
A.B.C.D/1.2.3.4} secondary ge?

no interface ge? ip-address
no interface ge? vlan vid ip-address
```

Table 113: Syntax Description

A.B.C.D/ bits	The IP address of the ge? interface. The /bits specifies the network mask in CIDR style.
A.B.C.D/ 1.2.3.4	The IP address of the ge? interface A.B.C.D is the dotted quad notation of the IP address 1.2.3.4 is the dotted quad notation of the subnet mask.
vlan vid	The VLAN to which the IP address should be assigned
secondary ge?	The name of the interface, which will serve as a secondary interface for the IP address. If the primary interface goes down and remains down for two seconds, the IP address will be moved to the secondary interface.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The specified interface IP address is configured to provide management access to the system over the gigabit ethernet interfaces.

Example

Use the `no interface ge? [vlan vid] ip-address` command to remove the IP address from the interface.

interface ha ip-address

To set the IP address and subnet mask for this system’s high-availability interface, use the `interface ha ip-address` command.

Syntax

```
interface ha ip-address {A.B.C.D/bits | A.B.C.D/1.2.3.4}
```

Table 114: Syntax Description

A.B.C.D/ bits	The IP address of the HA interface. The /bits specifies the network mask in CIDR style.
A.B.C.D/ 1.2.3.4	The IP address of the HA interface A.B.C.D is the dotted quad notation of the IP address 1.2.3.4 is the dotted quad notation of the subnet mask.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The HA features are used within a cluster of storage routers. Each member of the cluster communicates over the HA and management interfaces, exchanging heartbeats and other configuration information, allowing for failover in case of system problems.

The HA interface and the management interface must be on unique IP subnets. In a cluster, the HA interfaces for all storage routers should be on the same IP subnet.

After initial system configuration, use the `setup cluster` command to change the configuration of the storage router's high availability environment.

For storage routers deployed for iSCSI SAN interconnect or transparent SCSI routing, or standalone storage routers deployed for SCSI routing, the HA interface is optional.

Example

The following example assigns the IP address of *10.1.20.56/24* to the storage router's HA interface:

```
interface ha ip-address 10.1.20.56/24
```

interface mgmt

To set various operational parameters associated with the management interface, such as the speed and duplex mode, use the **interface mgmt** command.

```
interface mgmt autonegotiation
interface mgmt no autonegotiation [speed {10 | 100}] [duplex
{full | half}]
```

Table 115: Syntax Description

autonegotiation	Auto negotiation will always be used on this interface. Operational characteristics will automatically be negotiated with the partner.
speed 10	(Optional) The interface speed is fixed at 10 Mbps. Auto negotiation is not used.

Table 115: Syntax Description (Continued)

speed 100	(Optional) The interface speed is fixed at 100 Mbps. Auto negotiation is not used. If speed is not specified, the default is 100 Mbps.
duplex full	(Optional) The duplex setting is fixed at full. Auto negotiation is not used. If the duplex setting is not specified, the default is full duplex.
duplex half	(Optional) The duplex setting is fixed at half. Auto negotiation is not used.

Defaults

Auto negotiation is enabled.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to manually set a specific interface speed and duplex setting, if the partner is unable to auto negotiate these settings.

All storage routers in a cluster should be configured with the same interface-specific parameters, allowing failover to provide consistent performance characteristics. Use the **show interface mgmt** command to display current operating characteristics for the management interface.

Examples

The following example disables auto negotiation, and sets the interface speed to 10 Mbps, duplex full:

```
[HP SR2122-2] interface mgmt no autonegotiation speed 10 duplex full
```


Related Commands

Command	Description
<code>interface mgmt ip-address</code>	Specify the management interface IP address and subnet mask.
<code>show interface</code>	Display operational and configuration information for the specified interface or all interfaces.

interface mgmt ip-address

To set the IP address and network mask of the interface labeled MGMT on the front panel of the SR 2122 Storage Router, use the `interface mgmt ip-address` command. This address is used to manage the storage router via Telnet, the web-based GUI, or SNMP.

Syntax

```
interface mgmt ip-address {A.B.C.D/bits | A.B.C.D/1.2.3.4}
```

Table 116: Syntax Description

A.B.C.D/ bits	The IP address of the management interface. The /bits specifies the network mask in CIDR style.
A.B.C.D/ 1.2.3.4	The IP address of the management interface. A.B.C.D is the dotted quad notation of the IP address. 1.2.3.4 is the dotted quad notation of the subnet mask.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The management and HA interfaces must be on unique IP subnets. In a cluster, the management interfaces for all storage routers should be on the same IP subnet.

Examples

The following example assigns the IP address of *10.1.10.244/24* to the storage router's management interface:

```
interface mgmt ip-address 10.1.10.244/24
```

ip default-gateway

To add a gateway to the default route in the SR 2122 routing table, use the `ip default-gateway` command. To delete the gateway, use the `no` form of this command.

Syntax

```
ip default-gateway E.F.G.H  
no ip default-gateway [A.B.C.D]
```

Table 117: Syntax Description

<i>E.F.G.H</i>	The default gateway IP address
<i>A.B.C.D</i>	The IP address of the default route. The gateway to this route will be removed. (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

All IP interfaces in the storage router use the routing table to reach services and networks outside their local network. Other facilities, such as SNMP and connections to an NTP server or DNS servers, may also use the routing table. Use the `ip default-gateway` command to add a gateway to the default route in this table.

Examples

The following example adds the gateway *10.1.10.1* to the default route in the SR2122 routing table:

```
ip default-gateway 10.1.10.1
```

ip domain-name

To set the name of the storage router domain, use the `ip domain-name` command. To remove a domain name, use the `no` form of this command.

Syntax

```
ip domain-name name
no ip domain-name
```

Table 118: Syntax Description

name	The name of the storage router domain.
------	--

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `ip domain-name` command in conjunction with the `ip name-server` command. The storage router requires access to a DNS if any IP addresses are entered as host names via any of the SR2122 management interfaces, or if the SR 2122 management interface IP address is to be correlated with a DNS host name.

Note: If the DNS is outside the storage router management subnet, use the `ip route` command to add an appropriate gateway IP address to the SR 2122 routing table.

Examples

The following example assigns the domain name *mycompany.com* to the storage router.

```
ip domain-name mycompany.com
```

ip name-server

To set the IP address of the primary and optional secondary Domain Name Server (DNS), use the `ip name-server` command. To remove the settings for current domain name servers, use the `no` form of this command.

Syntax

```
ip name-server A.B.C.D [E.F.G.H]
no ip name-server
```

Table 119: Syntax Description

A.B.C.D	The IP address of a primary Domain Name Server, accessible by the storage router. A.B.C.D is the dotted quad notation of the IP address.
E.F.G.H	The IP address of a secondary DNS, accessible by the storage router. E.F.G.H is the dotted quad notation of the IP address. (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The storage router requires access to a DNS if any IP addresses are entered as host names via any of the SR 2122 management interfaces, or if the SR 2122 management interface IP address is to be correlated with a DNS host name. To use the services of a DNS, you must also assign a domain name to the storage router via the `ip domain-name` command.

Note: If the DNS is outside the storage router management subnet, use the `ip route` command to add an appropriate gateway IP address to the SR 2122 routing table.

Examples

The following example assigns the domain name *abc123.com* to the storage router and assigns the IP address of the primary DNS to *10.1.40.243* and the secondary DNS to *10.1.50.249*:

```
ip domain-name abc123.com
ip name-server 10.1.40.243 10.1.50.249
```

ip route

To add a static route to the SR 2122 routing table, use the `ip route` command. The specified IP address is accessed via the gateway specified in the command. To remove a static route from the routing table, use the `no` form of this command.

Syntax

```
ip route {A.B.C.D/bits | A.B.C.D/1.2.3.4} E.F.G.H
[administrative-distance]
no ip route {A.B.C.D/bits | A.B.C.D/1.2.3.4} [E.F.G.H]
```

Table 120: Syntax Description

A.B.C.D/bits	The IP address of the static route. A.B.C.D is the dotted quad notation of the IP address. The /bits specifies the subnet mask in CIDR style.
A.B.C.D/1.2.3.4	The IP address of the static route. A.B.C.D is the dotted quad notation of the IP address. 1.2.3.4 is the dotted quad notation of the subnet mask.
E.F.G.H	The gateway IP address through which the static route (A.B.C.D/bits or A.B.C.D/1.2.3.4) is accessed
administrative-distance	The administrative distance for the route. Valid values are 0 to 255 inclusive. The default administrative distance is 1. (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

All IP interfaces in the storage router use the routing table to reach services and networks outside their local network. Other facilities, such as SNMP and connections to an NTP server or DNS servers, may also use the routing table. Use the `ip route` command to set routes for servers or networks outside the local networks associated with the storage router's IP interfaces. To add a default route issue the command "`ip route 0.0.0.0/0 A.B.C.D`".

Use the `show ip route` command to display the routing table. Use the `show route` command to display all the default routes, included the routes that have been configured but not added to the routing table.

The administrative distance is used to determine which route to install in the routing table when there are multiple routes to the same destination. The default administrative distance for static routes is 1; the administrative distance for dynamic routes created by RIP is 120. The route with the lower administrative distance is installed in the routing table (as long as the interface used by the route is up).

By default, a static route will always override a dynamic route learned by RIP. To modify this behavior, change the administrative distance of a static route to a value greater than 120.

A route is not added to the routing table until the associated interface is configured. The CLI displays an informational message if a route is added for an IP address that is not yet configured.

Examples

The following command adds a unique route for the Gigabit Ethernet interface, specifying the subnet mask in dotted quad notation:

```
ip route 10.1.30.0/255.255.255.0 10.1.10.1
```

The following command adds a unique route for IP address 10.1.40.0, using gateway 10.1.10.10, which is not yet on a locally connected network. The message indicates that the route has been configured but has not yet been made operational in the storage router.

```
ip route 10.1.40.0/24 10.1.10.10
Oct 25 19:25:17: %UI-4-NMREEO1: Gateway 10.1.10.10 used by route
10.1.40.0/24 is currently unreachable
```

The following command adds a unique route for IP address *10.1.20.0* with an administrative distance of *130*, in the routing table. If RIP is enabled for the storage router, the route can be overridden by a dynamically learned route.

```
ip route 10.1.20.0/24 10.1.10.10 130
```

isns enable

To enable communications and client registrations with an iSNS server, use the **isns enable** command. To disable iSNS communications and services, use the **no** form of this command.

```
isns enable {tcp | udp} server A.B.C.D [port port-number]
no isns enable
```

Table 121: Syntax Description

tcp	Keyword, indicating the iSNS server expects client registrations and other communications via TCP.
udp	Keyword, indicating the iSNS server expects client registrations and other communications via UDP.
server	Keyword, identifying the following IP address as the location of the iSNS server.
A.B.C.D	The IP address of the iSNS server.
port port-number	(Optional) The iSNS listening port. If unspecified, the port number defaults to 3205.

Defaults

The default iSNS listening port is 3205.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced.

User Guidelines

Internet Storage Name Service (iSNS) is an IETF standard that facilitates scalable configuration and management of iSCSI and FC storage devices in an IP network by providing a set of services comparable to that available in FC networks. Using the iSNS, each storage device subordinates its discovery and management responsibilities to the iSNS server.

The storage router functions as an iSNS client. SCSI routing instances are registered as iSNS entities, targets are registered as storage nodes, and SCSI routing instance server interface IP addresses are registered as network portals with the iSNS server. The storage router management interface IP address is registered as an attribute of the SCSI routing instance iSNS entity.

iSNS servers may use TCP or UDP protocol for client registrations and other communications. Use the **isns enable** command to identify the iSNS server and communications protocol to the storage router.

Examples

The following example enables iSNS communications and client registrations using TCP protocol to the iSNS server at 10.1.70.43, using the default port 3205:

```
[HP SR2122-2]# isns enable tcp server 10.1.70.43
```

The following example enables iSNS communications and client registrations using UDP protocol to the iSNS server at 10.1.20.21, using port 1443:

```
[HP SR2122-2]# isns enable udp server 10.1.20.21 port 1443
```

The following examples disables all iSNS communications and client registrations:

```
[HP SR2122-2]# no isns enable
```


Related Commands

Command	Description
<code>debug isns</code>	Enable tracing of iSNS Protocol Data Units (PDUs).
<code>isns refresh</code>	Force a refresh of the iSNS server with device registrations.
<code>show debug isns</code>	Display iSNS PDU traced contents and statistics.
<code>show isns</code>	Display iSNS configuration information, objects, or operational statistics.

isns refresh

To force a refresh of the iSNS server with device registrations, use the **isns refresh** command.

```
isns refresh
```

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced.

Usage Guidelines

Use the **isns refresh** command to manually force the storage router to reregister all iSNS entities, storage nodes and network portals. Use the **show isns objects** commands to view the iSNS client and device registrations.

Examples

The following example refreshes the client and device registrations for the storage router named HP SR2122-2:

```
[HP SR2122-2]# isns refresh
```

Related Commands

Command	Description
debug isns	Enable tracing of iSNS Protocol Data Units (PDUs).
isns enable	Enable communications and client registrations with an iSNS server.
show debug isns	Display iSNS PDU traced contents and statistics.
show isns	Display iSNS configuration information, objects, or operational statistics.

ping

To verify communication with another storage router or system in the network, use the `ping` command.

Syntax

```
ping {ip-address / servername} [numpkts npkts] [size sn]
```

Table 122: Syntax Description

ip-address	The IP address of another system or storage router.
servername	The name of another server. The storage router must have be configured to use the services of a Domain Name Server (DNS).
numpkts	The keyword indicating the maximum number of pings that may be sent (Optional)
npkts	The maximum number of pings. The default value is five . Range is 1 to MAX integer (Optional)
size	The keyword indicating the size of each ping packet (Optional)
sn	The size of each packet, in bytes. The default is 64 bytes. Range is 1-4096 (Optional)

Defaults

The default setting is to attempt **five 64-byte pings**.

Command Modes

Administrator or Monitor. The optional **numpkts** and **size** keywords are not available in Monitor mode.

Usage Guidelines

Use this command to verify that TCP/IP communication path to another storage router or system in the network. Some debugging is done by technicians by varying the packet size. The packet-size does not include the additional 8 bytes for the ICMP header.

Examples

The following example attempts to verify the communication path to the IP address *10.1.30.17*, using the default size and maximum number of packets:

```
ping 10.1.30.17
ping 10.1.30.17
Sending up to 5 64-byte pings to 10.1.30.17 ....
host 10.1.30.17 is reachable!
The following example attempts to reach the IP address 10.1.30.17 by sending
3-20 byte packets:
ping 10.1.30.17 numpkts 3 size 20
ping 10.1.30.17 numpkts 3 size 20
Sending up to 3 20-byte pings to 10.1.30.17 ....
host 10.1.30.17 is unreachable!
```

restrict console

To enable password checking on the storage router console interface, use the `restrict console` command. The Administrator-mode and Monitor-mode passwords are required when accessing the storage router via a console connected to the RS-232 port. To disable password checking on the console interface, use the `no` form of this command.

Syntax

```
restrict console
no restrict console
```

This command has no arguments or keywords.

Defaults

Passwords are disabled on the console interface.

Command Modes

Administrator.

Usage Guidelines

Use this command if you need to restrict access to the storage router's console interface.

Examples

The following example enabled password checking on the storage router's console interface:

```
restrict console
```

restrict

To close access to the specified interface via FTP, HTTP, SNMP, or Telnet, use the `restrict` command. To allow FTP, HTTP, SNMP, or Telnet access, use the `no` form of this command.

Syntax

```
restrict all service
restrict interface {service | all}
no restrict all [service]
no restrict interface [service | all]
```

Table 123: Syntax Description

<code>interface (?)</code>	Restricts access to the specified interface
<code>all</code>	Restricts all interface or all services
<code>service</code>	Restricts access via the specified service or protocol

Defaults

The following are factory default settings:

- FTP using port 21 is restricted on all interfaces
- HTTP using port 80 is allowed on the management and HA interfaces. It is restricted on the Gigabit Ethernet interface. (HTTP access cannot be restricted on the management or HA interface.)
- Login using port 513 is restricted on all interfaces.
- SNMP using port 161 is allowed on the management interface. It is restricted on the HA and Gigabit Ethernet interfaces.
- SSH using port 22 is allowed on the management interface only. It is restricted on the HA and Gigabit Ethernet interfaces.
- SSL using port 443 is restricted on all interfaces.
- Telnet using port 23 is allowed on the management interface only. It is restricted on the HA and Gigabit Ethernet interfaces.

Table 124: Default settings

	telnet (23)	http (80)	snmp (161)	ftp (21)	ssl (443)	rlogin (513)
console	no pw required					
MGMT	monitor pw required	pw required	open	no access	no access	no access
HA	no access	pw required	no access	no access	no access	no access
GbE	no access	no access	no access	no access	no access	no access

Command Modes

Administrator.

Usage Guidelines

Use the `restrict interface` command to restrict unauthorized access to storage router interfaces. Login access is only available under direct instruction from TAC. Use the `show restrict` command to display the current interface and service restrictions.

Table 125: restrict Interface-ID

Keyword	Description
mgmt	The storage router management interface. HTTP access cannot be disabled for the management interface.
ha	The storage router HA interface. HTTP access cannot be disabled for the HA interface.
ge?	The storage router Gigabit Ethernet interface (including all logical interfaces created by associating a VLAN with a Gigabit Ethernet IP address for a SCSI routing instance).

You can restrict access to the storage router interfaces by the services or protocols:

Table 126: restrict interface Service

Keyword	Description
ftp	File Transfer Protocol. FTP access is restricted on all interfaces, by default.
http	Hypertext Transfer Protocol. HTTP access is available on the management and HA interfaces, by default.
rlogin	Remote login on port 513. If rlogin is enabled for an interface, the setting is only valid until the storage router is restarted. The rlogin setting is not retained across a storage router restart; rlogin returns to a restricted state for all interfaces. Rlogin is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.
ssh	Secure Shell. SSH can be used as a replacement for Telnet and remote login. SSH is enabled on the management interface by default; it is restricted on all other interfaces. The SSH service is started, by default. Use the no ssh enable command to stop the SSH service (disabling access via SSH) without changing the restrict settings.

Table 126: restrict interface Service (Continued)

Keyword	Description
snmp	Simple Network Management Protocol. SNMP is enabled on the management interface by default.
ssl	Secure Socket Layer. SSL is restricted on all interfaces by default.
telnet	Telnet. Telnet access is enabled on the management interface by default; it is restricted on all other interfaces. The Telnet server is started by default. Use the no telnet enable command to stop the Telnet server (disabling access via Telnet) without changing the restrict settings.

To access the GUI using an SSL connection, enable SSL on the appropriate interface and change the URL to use “https” instead of “http.”

To completely disable the GUI, restrict HTTP access to all interfaces.

Examples

The following example restricts HTTP access on the Gigabit Ethernet interface, *ge2*:

```
restrict ge2 http
```

The following example enables SSL on the management interface.

```
no restrict mgmt ssl
```

scsirouter serverif

To assign a Gigabit Ethernet and IP address to the named SCSI routing instance, use the `scsirouter serverif` command. The specified interface allows IP hosts and FC server instances access to storage devices.

Syntax

```
scsirouter name serverif ge? {A.B.C.D/bits | A.B.C.D/1.2.3.4}
scsirouter name serverif ge? {A.B.C.D/bits | A.B.C.D/1.2.3.4}
secondary ge?

scsirouter name serverif ge? vlan vid {A.B.C.D/bits |
A.B.C.D/1.2.3.4}

scsirouter name serverif ge? vlan vid {A.B.C.D/bits |
A.B.C.D/1.2.3.4} secondary ge?
```

Table 127: Syntax Description

name (?)	The name of the SCSI routing services to which you are adding the Gigabit Ethernet interface
serverif ge?	The name of the interface. When you type the <code>scsirouter serverif</code> command, followed by <code>?</code> , the CLI lists the interfaces available. You cannot specify a nonexistent interface.
A.B.C.D/ bits	The IP address of the named interface. If the keyword vlan is used, the IP address is part of the specified VLAN. A.B.C.D is the dotted quad notation of the IP address. The <code>/bits</code> specifies the subnet mask in CIDR style.
A.B.C.D/ 1.2.3.4	The IP address of the named interface. If the keyword vlan is used, the IP address is part of the specified VLAN. A.B.C.D is the dotted quad notation of the IP address. 1.2.3.4 is the dotted quad notation of the subnet mask.
vlan vid	The keyword and the virtual LAN identifier
secondary ge?	The name of the interface which will serve as a secondary interface for the IP address. If the primary interface goes down and remains down for two seconds, the IP address will be moved to the secondary interface.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The specified interface IP address is configured on IP hosts and FC server instances requiring IP access to storage through the SR 2122 Storage Router.

Each SCSI routing instance requires these elements:

- The *serverif* element assigns an interface and IP address for use by the IP hosts or FC server instances requiring IP access to storage devices.
- The *target* element is a complex item that specifies the mapping between LUNs on the storage devices and the host systems.

The `scsirouter serverif vlan` command is used to associate a VLAN with a SCSI routing instance. All traffic using the specified Gigabit Ethernet interface will be considered as part of the VLAN; all IP hosts and accessing storage through the storage router using the specified Gigabit Ethernet interface IP address must connect as part of the specified VLAN.

When the SCSI routing instance is started, a logical interface is created with a name that incorporates the VID and the physical interface, such as *VLAN100ge2*. This logical interface can be displayed via the `show interface` command and can be used when adding static routes to the system.

Examples

The following command adds the Gigabit Ethernet interface *ge2*, with the IP address *10.1.10.255/24*, to the SCSI routing instance named *fool*.

```
scsirouter fool serverif ge2 10.1.10.255/24
```

The following command adds the Gigabit Ethernet interface *ge2* as VLAN ID *45*, with IP address *11.1.30.255/24*, to the SCSI routing instance *fool*:

```
scsirouter fool serverif ge2 vlan 45 11.1.30.255/24
```

show debug isns

To display iSNS PDU traced contents and statistics, use the **show debug isns** command.

```
show debug isns trace [first nn | last nn]
show debug isns trace hex [ascii] [first nn | last nn]
show debug isns trace stats
```

Table 128: Syntax Description

trace	Display the entire decoded trace buffer.
trace stats	Display iSNS PDU trace statistics and configuration information.
trace hex	Display the iSNS PDU trace buffer in hex.
ascii	(Optional) Display iSNS PDU trace in hex and ASCII.
first nn	(Optional) Display the specified number of PDUs from the start of the trace buffer.
last nn	(Optional) Display the specified number of PDUs from the end of the trace buffer.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced.

To enable iSNS PDU trace facilities for debugging purposes, use the **debug isns** command. The **show debug isns** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Note: iSNS PDU tracing must be disabled before the trace buffer can be displayed.

Examples

The following example disables iSNS PDU tracing and then displays the full contents of the trace buffer:

```
[HP SR2122-2_PR]# no debug isns trace enable
[HP SR2122-2_PR]# show debug isns trace
1: 10.1.51.125:3542 -> 10.1.0.194:3205, len 336, time 0.000
   PDU: ver=1 funcId=1 (DevAttrReg) pduLen=324 flags=9c00
   (Client,Replace,First,Last) tid=579 sid=0
   TLV: IScsiName : iqn.1987-05.com.cisco:00.2dad14af2d36.t1
        EntityId : iqn.1987-05.com.cisco:06.cddb3e6f6fcc.g1
        Delimiter
        EntityId : iqn.1987-05.com.cisco:06.cddb3e6f6fcc.g1
        EntityProto : 2
        MgmtIpAddr : 10.1.70.125
        IScsiName : iqn.1987-05.com.cisco:00.2dad14af2d36.t1
        IScsiNodeType : 1
        IScsiAlias : t1
        PortalIpAddr : 10.1.80.1
        PortalTcpUdpPort : 3260
        PortalGroupTag : 1
```

Related Commands

Command	Description
<code>debug isns</code>	Enable tracing of iSNS Protocol Data Units (PDUs).
<code>isns enable</code>	Enable communications and client registrations with an iSNS server.
<code>isns refresh</code>	Force a refresh of the iSNS server with device registrations.
<code>show isns</code>	Display iSNS configuration information, objects, or operational statistics.

show debug interface ge?

To display IP packet trace buffer statistics and contents, use the **show debug interface ge?** command.

```
show debug interface ge? trace stats
```

```
show debug interface ge? trace [first nn | last nn]
```

```
show debug interface ge? trace hex [ascii] [first nn | last nn]
```

Table 129: Syntax Description

ge?	Display IP trace information for the specified Gigabit Ethernet interface. When you type the show debug interface ge? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
trace	Display the entire trace buffer, in hex.
trace stats	Display packet trace statistics and configuration information.
first nn	(Optional) Display the specified number of packets from the start of the trace buffer.
last nn	(Optional) Display the specified number of packets from the end of the trace buffer.
trace hex	Display packet trace in hex.
ascii	(Optional) Display packet trace in hex and ASCII.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.5.1	This command was introduced for the HP SR2122.
3.2.1	This command was introduced for the HP SR2122-2.
3.3.1	The hex and ascii keywords were added.

Usage Guidelines

To enable IP packet trace facilities for debugging Gigabit Ethernet interfaces, use the **debug interface ge?** command. The **show debug interface ge?** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Note: IP packet tracing must be disabled on the interface before the trace buffer can be displayed.

Examples

The following example disables IP packet tracing on the interface *ge1* and then displays the full contents of the trace buffer:

```
[HP SR2122-2_PR]# no debug interface ge1 trace enable
[HP SR2122-2_PR]# show debug interface ge1 trace
1: RX, len 60, time 0.000
0000: 01 00 0c cc cc cc 00 08 7c 3c 3d 85 00 28 aa aa
0010: 03 00 00 0c 20 04 01 00 01 00 0b 64 61 76 65 74
0020: 68 6f 00 02 00 05 81 00 03 00 05 a5 00 04 00 0a
0030: 00 08 7c 3c 3d 85 00 00 00 00 00 00
```

Related Commands

Command	Description
<code>debug interface ge?</code>	Enable IP packet tracing for the specified Gigabit Ethernet interface.

show ip

To display information about the SR 2122 network, including a variety of protocol stack statistics, use the `show ip` command.

Syntax

```
show ip {arp | hosts | route | tcp | udp}
show ip [icmp | route | tcp | udp] stats
```

Table 130: Syntax Description

arp	Displays the ARP table
hosts	Displays all known hosts on the SR 2122 IP network
route	Displays the system route table
tcp	Displays active TCP connections
udp	Displays system UDP activity
icmp stats	Displays ICMP-related network statistics
route stats	Displays route-related network statistics
tcp stats	Displays TCP-related network statistics
udp stats	Displays UDP-related network statistics
stats	Display all IP-related network statistics

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show ip` command with the **stats** keyword to display operational network statistics related to the specified protocol. The information displayed depends on the type of protocol specified.

- Use the **arp** keyword to display the ARP table.
- Use the **hosts** keyword to display all known hosts on the SR 2122 IP network.
- Use the **route** keyword to display the SR 2122 system routing table, including network and host routes. **0.0.0.0/32** is the default route.
- Use the **tcp** keyword to display active TCP connections, including the storage router web server and other tasks.
- Use the **udp** keyword to display User Datagram Protocol (UDP) activity on the system.

Examples

The following is an example output from the `show ip stats` command:

```
show ip stats
show ip stats
Total Packets                131784
Bad Checksum                 0
Packet too Short             0
Not Enough Data              0
Bad Header Length            0
Bad Packet Length            0
Fragments Received           0
Fragments Dropped            0
Fragments Timed Out          0
Packets Forwarded            0
Destination Unreachable      1604
Redirected Packets            0
Unknown Protocol             17
Out of Buffers                0
Packets Reassembled          0
Fragments Sent               0
No Route                     0
Generic Drop                  0
```

show isns

To display iSNS configuration information, objects, or operational statistics, use the **show isns** command.

```
show isns [objects | stats]
```

Table 131: Syntax Description

objects	Display the status of the storage router's iSNS objects.
stats	Display iSNS operational statistics. This display shows statistics accumulated since the storage router was last restarted or statistics were last cleared, whichever is more recent.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.4.1	This command was introduced.

Usage Guidelines

Internet Storage Name Service (iSNS) is an IEFT standard that facilitates scalable configuration and management of iSCSI and FC storage devices in an IP network by providing a set of services comparable to that available in FC networks. Using the iSNS, each storage device subordinates its discovery and management responsibilities to the iSNS server.

The storage router functions as an iSNS client. SCSI routing instances are registered as iSNS entities, targets are registered as storage nodes, and SCSI routing instance server interface IP addresses are registered as network portals with the iSNS server. The storage router management interface IP address is registered as an attribute of the SCSI routing instance iSNS entity.

Use the **show isns** command with no keywords to display the IP address of the iSNS server and other configuration information. Use the **objects** keyword to display information about the storage router's registered entities and associated attributes, nodes and portals. Use the **stats** keyword to display current iSNS operational statistics.

Examples

The following is output from the **show isns** command:

```
[HP SR2122-2]# show isns
Status      Server          Port  Proto Connection State
-----
enabled    10.1.0.194        3205  TCP    connected
```

Table 132 describes the fields shown in the display:

Table 132: Description of Fields in the “show isns” Command Output

Field	Description
Status	Indicates if iSNS client registrations and communications are enabled for the storage router.
Server	The IP address of the iSNS server.
Port	The port used for iSNS listening.
Proto	The communications protocol, TCP or UDP.
Connection State	Indicates if the storage router is currently connected to the iSNS server.

The following is output from the **show isns objects** command:

```
[HP SR2122-2]# show isns objects
Entity iqn.1987-05.com.cisco:06.1a9a06c81a0c.sr1: Proto=iSCSI
Mgmt=10.1.70.101 RegPeriod=900 Status=Registered
  Node iqn.1987-05.com.cisco:00.10ed3fb46188.t1: Type=Target
Alias=t1 Status=Registered
  Node iqn.1987-05.com.cisco:00.d7f351c0d5d0.t2: Type=Target
Alias=t2 Status=Registered
  Portal 10.1.50.101:3260: PortalGroupTag=1 Status=Registered
```

Table 133 describes the entities and attributes shown in the display:

Table 133: Description of Entities and Attributes in the “show isns objects” Command Output

Field	Description
Entity	The SCSI routing instance. The instance name is shown at the end of the iSCSI Name. Entities may contain both Nodes and Portals.
Proto	The type of protocol involved. SCSI routing instances use iSCSI protocol.
Mgmt	The IP address of the management interface for the storage router running the SCSI routing instance.
RegPeriod	The maximum period, in seconds, that the registration is maintained by the iSNS server without the receipt of an iSNS message from the storage router (iSNS client) that registered the entity.
Status	The status of the iSNS registration for the entity.
Node	The iSNS Storage Node object associated with the iSNS Entity. The Node is represented by the iSCSI Name of the target associated with the SCSI routing instance.
Type	The type of node.
Alias	The name of the SCSI routing instance target.
Status	The status of the iSNS registration for the node.
Portal	The IP address of the SCSI routing instance server interface. The iSCSI port number is shown at the end of the IP address.
PortalGroupTag	The Portal Group Tag (PGT) associated with the Node and the Portal. If non-null, the PGT indicates that the associated Portal provides access to the associated Node in the Entity. All Portals that have the same PGT value for a specific Node allow coordinated access to that storage.
Status	The status of the iSNS registration for the Portal.

The following is output from the **show isns stats** command:

```
[HP SR2122-2]# show isns objects
tcpConnAttempts = 34
udpRetrans = 0
connResets = 0
devRegFailures = 0
serverBusy = 0
txPdus = 34
txDevRegPdus = 1
txDevDeregPdus = 0
txDevAttrQryPdus = 33
txPduBytes = 4768
txPduErrors = 0
rxPdus = 34
rxDevRegRspPdus = 1
rxDevDeregRspPdus = 0
rxDevAttrQryRspPdus = 33
rxPduBytes = 3676
rxPduErrors = 0
rxPdusBadSrc = 0
rxPdusShortHdr = 0
rxPdusShortPayload = 0
rxPdusNoStatus = 0
rxPdusNoTidMatch = 0
rxPdusBadFuncId = 0
```

[Table 134](#) describes the fields shown in the display:

Table 134: Description of Fields in the “show isns stats” Command

Field	Description
tcpConnAttempts	The number of times the storage router has attempted to connect to the iSNS server.
udpRetrans	The number of times the storage router has retransmitted UDP messages to the iSNS server.
connResets	The number of times the iSNS server connection has been reset.
devRegFailures	The number of iSNS registration failures.
serverBusy	The number of times the iSNS server has returned busy.
txPdus	The total number of iSNS Protocol Data Units (PDUs) transmitted by the storage router.
txDevRegPdus	The number of device registration PDUs transmitted by the storage router.
txDevDeregPdus	The number of device deregistration PDUs transmitted by the storage router.

Table 134: Description of Fields in the “show isns stats” Command (Continued)

Field	Description
txDevAttrQryPdu	The number of device attribute query PDUs transmitted by the storage router.
txPduBytes	The total number of bytes transmitted in all PDUs.
txPduErrors	The total number of PDU transmit errors.
rxPdu	The total number of iSNS PDUs received by the storage router.
rxDevRegRspPdu	The number of device registration response PDUs received by the storage router.
rxDevDeregRspPdu	The number of device deregistration response PDUs received by the storage router.
rxDevAttrQryRspPdu	The number of device attribute query response PDUs received by the storage router.
rxPduBytes	The total number of bytes received in all PDUs.
rxPduErrors	The total number of PDU receive errors.
rxPduBadSrc	The total number of PDUs received with bad source information.
rxPduShortHdr	The total number of PDUs received with a short header.
rxPduShortPayload	The total number of PDUs received with a short payload.
rxPduNoStatus	The number of PDUs received with no status.
rxPduNoTidMatch	The number of PDUs received with no matching transaction IDs.
rxPduBadFuncId	The number of PDUs received with bad function IDs.

Related Commands

Command	Description
<code>debug isns</code>	Enable tracing of iSNS Protocol Data Units (PDUs).
<code>isns enable</code>	Enable communications and client registrations with an iSNS server.
<code>isns refresh</code>	Force a refresh of the iSNS server with device registrations.
<code>show debug isns</code>	Display iSNS PDU traced contents and statistics.

show route

To display all routes that have been configured, including those that have not been added to the routing table because the associated interface is not yet configured, use the `show route` command.

Syntax

```
show route
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use this command to display all routes that have been configured for the storage router, including routes that have been configured but have not been added to the routing table. Use the `show ip route` command to display the entire SR 2122 routing table.

A route is not added to the routing table until the associated interface is configured.

Examples

The following is example output from the `show route` command:

```
show route
ip route 0.0.0.0/24 10.1.10.1
ip route default 10.1.10.1
```

Logging Commands

11

This section describes all the CLI commands related to the event and error logging feature in the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

clear log

To clear the SR 2122 Storage Router log file of all entries, issue the `clear log` command.

Syntax

```
clear log
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

You may want to clear the log file if it is too large or if you are going to perform testing and want to be sure the log file only reflects information from the testing session. To copy the log file to or from a SR 2122 to another location use the `copy tftp` command.

The `clear conf` command also clears all entries from the storage router log file. Archiving the log files on the SR 2122 currently is not supported.

Examples

The following examples clear all entries from the storage router log file:

```
clear log
```


logging syslog

To log messages to a syslog server, use the `logging syslog` command. To stop logging messages to syslog servers, use the `no` form of this command.

Syntax

```
logging syslog A.B.C.D
no logging syslog
```

Table 135: Syntax Description

A.B.C.D	The IP address of the server to be used as the syslog server
---------	--

Defaults

Logging to a syslog sever is disabled by default.

Command Modes

Administrator.

Usage Guidelines

This command identifies a syslog server host to receive logging messages.

- Use the `no logging syslog` command to disable logging to a syslog server.
- Use the `show system` command to display syslog server and facility information.
- Use the `save system` command to save remote logging configuration information.

Examples

The following example identifies the syslog server as the server at IP address *10.1.1.144*:

```
logging syslog 10.1.1.144
```

logging

To add a log route entry, use the `logging` command.

Syntax

```
logging level <log_level> from <name> to [all none console vty  
logfile rslog]  
  
logging #<entry> level <log_level> from <name> to [all none  
console vty logfile rslog]  
  
delete logging level <log_level> from <name>  
  
delete logging #<entry>
```

Table 136: Syntax Description

entry	Adds or deletes a specified entry in the logging table
log_level	Limits logging to messages of a specified level or lower levels
name	Unique facility name
all	Logs to all destinations
none	Logs to no destinations
console	Logs to serial console destination
vtty	Logs to virtual terminal destination
logfile	Logs to log file destination
rslog	Logs to remote log destination

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

When a new log route entry is added without a specified entry position, it is appended to the list of entries.

When a log message arrives it is mapped to its destination by traversing the list of log route entries from first to last. The entries are compared first by level, then by facility name. When the first match is found the log message is sent to the corresponding destinations.

Examples

The following example appends a log route entry containing the facility name *UI* with notification level set to *error* and the list of destinations set to *console* and *logfile*.

```
logging level error from ui to console logfile
```

logging on

To temporarily enable or disable event messages, use the `logging on` or `no logging on` command.

Syntax

```
logging on  
no logging on
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

None.

Examples

None.

show logging

To display event logging settings or to display contents of the log file, use the `show logging` command.

Syntax

```
show logging [all | last nn] [match text] | size
```

Table 137: Syntax Description

<code>all</code>	Displays all log file entries (Optional)
<code>last nn</code>	Displays the last nn lines from the current storage router log file (Optional)
<code>match text</code>	Displays all entries that match the specified string. String matching is case-sensitive. Also can specify a regular expression like "name[0-9][a-zA-Z]" (Optional)
<code>size</code>	Displays the number of messages in the log file and the size of the logfile, in bytes (Optional)

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show logging` command to display the current event logging settings.

Use the `match string` parameters to display messages matching the specified string. You can search the entire log file for matching messages or restrict the search to the last *nn* number of messages.

Examples

The following is an example output from the `show logging` command:

```
show logging
Logging is enabled
Index      Level      Priority    Facility    Route
1          notice    5          all         all
2          info      6          all         logfile
3          debug     7          UI          vty
show logging last 2
Jul 15 15:16:33: %UI-6-CCEMCS: Executed command "show logging"
return
code is 0
Jul 15 15:18:29: %UI-6-CCEMCS: Executed command "show logging last
"2"
return code is 0
```

show logging

SCSI Commands

12

This section describes all the CLI commands related to setting and monitoring the SCSI protocol. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

scsirouter lun reset

To specify that `LUN reset` rather than `clear task` commands will be sent to storage devices opened by the specified SCSI routing instance, use the `scsirouter lun reset` command.

Syntax

```
scsirouter name lun reset {yes | no}
```

Table 138: Syntax Description

<i>name</i>	The name of the SCSI routing instance. The specified SCSI routing instance must be running on a storage router in a cluster.
<i>yes</i>	Specifies that “lun reset” will be sent to storage devices when they are opened
<i>no</i>	Species that “clear task” will be sent to storage devices when they are opened

Defaults

The default is to send `clear task` command to storage devices.

Command Modes

Administrator.

Usage Guidelines

It is preferable to send `lun reset` commands if the device supports them. The specified SCSI routing instance must be running on a storage router in a cluster.

Examples

The following example enables “LUN resets” to all storage devices opened by the SCSI routing instance *fool*:

```
scsirouter fool lun reset yes
```


scsirouter reserveproxy

To configure the SCSI routing instance to use SCSI Reserve / Release commands and to specify whether these commands are forwarded to the storage target, use the `scsirouter reserveproxy` command.

Syntax

```
scsirouter name reserveproxy disable
scsirouter name reserveproxy enable passthru {yes | no}
```

Table 139: Syntax Description

<i>name</i> (?)	The name of the SCSI routing instance
enable passthru <i>yes</i>	Configure the SCSI routing instance to use SCSI <code>reserve</code> and <code>release</code> commands and enable forwarding of these commands to storage devices.
enable passthru <i>no</i>	Configure the SCSI routing instance to use SCSI <code>reserve</code> and <code>release</code> commands but disable forwarding of these commands to storage devices
<i>disable</i>	Disables the reserve proxy feature for the named SCSI routing instance

Defaults

Reserve proxy passthru is disabled.

Command Modes

Administrator.

Usage Guidelines

The SCSI Reserve / Release command allows an initiator to reserve the storage device for its own use. Attempts to access the storage device from other initiators are rejected until the first initiator releases the storage device. If this feature is enabled using the `scsirouter reserveproxy` command, the storage router keeps track of the reserved status of target LUNs and returns the appropriate SCSI command status to other initiators that issue SCSI commands to that target LUN.

The functionality does not apply to operating systems (such as Windows NT) which do not utilize the SCSI Reserve command.

Examples

The following example configures the SCSI routing instance *fool* to use SCSI reserve and release commands, and enables forwarding of these commands to storage devices:

```
scsirouter fool reserveproxy enable passthru yes
```

scsirouter target accesslist

To associate the named access list with the specified target, use the `scsirouter target accesslist` command.

Syntax

```
scsirouter name target {name | all} accesslist {name | all | none}
```

Table 140: Syntax Description

name (?)	The name of the SCSI routing instance to which this target belongs
target name (?)	The name of the storage target to associate with this access list. The target must already exist.
target all	Associates all targets with the named access list

Table 140: Syntax Description (Continued)

<code>accesslist</code> <i>name</i>	The name of the access list to associate with this storage target
<code>accesslist</code> <i>none</i>	Prevents any new connections and logins to this target from any IP hosts and FC server instances. This is effectively “no access.”
<code>accesslist</code> <i>all</i>	Allows connections and logins for the specified target from all IP hosts and FC server instances. This is effectively “open access.”

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

An access list specifies the IP addresses of IP hosts and FC server instances allowed to access the associated storage target through the storage router. Access lists are associated with specific storage targets. Use the `target all` form of this command to create an association between the specified access list and all targets.

Existing connections and logins are not affected by an access list change. However, if there are existing connections, the storage router issues a warning message with that information in response to this command.

Use the reserved access list name `none` to remove any access list associations for the specified target. This effectively prevents access to this storage target from any IP hosts or FC server instances.

Use the reserved access list name `all` to allow access to this storage target from any IP hosts or FC server instances. This is effectively “open access.”

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example creates an association between the storage target *webserver4* (accessed via SCSI routing instance *foo*) and the access list *webserver2*.

```
scsirouter foo target webserver4 accesslist webserver2
```

scsirouter target description

To add a description to the named target, use the `scsirouter target description` command.

Syntax

```
scsirouter name target name description "text"
```

Table 141: Syntax Description

<i>name</i> (?)	The name of the SCSI routing instance to which this target belongs
target <i>name</i> (?)	The name of the storage target
description "text"	User-defined identification information associated with this storage target. If the description contains spaces, enclose the string in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Target description information is an optional attribute of a SCSI routing instance. Use the `show scsirouter` command to display target description information.

Examples

The following example adds a description to the storage target *webserver4*, accessed through the SCSI routing instance *foo*:

```
scsirouter foo target webserver4 description
```

scsirouter target {enabled | disabled}

To allow or disallow connections and logins for the named target, use the `scsirouter target` command.

Syntax

```
scsirouter name target {name | all} {enabled | disabled}
```

Table 142: Syntax Description

<i>name (?)</i>	The name of the SCSI routing instance to which this target belongs
target <i>name (?)</i>	The name of the storage target
target <i>all</i>	Allows connections for all targets of this SCSI routing instance to be enabled or disabled
<i>enabled</i>	Allows connections and logins for the named target or for all targets, of the specified SCSI routing instance
<i>disabled</i>	Prevents new connections and logins for the named target or for all targets, of the specified SCSI routing instance

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

When you add a target to a SCSI routing instance, it is enabled by default. However, no access list is associated with the target, effectively preventing any access to the storage target from any IP hosts or FC server instances. When you

associate an access list with a target, the specified connections and logins are allowed. Use the `scsirouter target` command **enabled** or **disabled** keywords to control access without changing the target access list association.

Existing connections and logins are not affected by the **disabled** keyword, but future connections and logins are not allowed. If existing IP hosts and FC server instances are connected, the storage router issues a warning message with that information in response to this command.

Use the reserved target name `all` to enable or disable connections for all targets of this SCSI routing instance.

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example enables connections for all targets of the SCSI routing instance `scsiA`.

```
scsirouter scsiA target all enable
```

scsirouter target {serial | lunwwn | wwpn} #?

To use an index method of mapping a logical target (or a logical target and LUN combination) to storage, use the `scsirouter target {serial | lunwwn | wwpn} #?` command. This command creates an indexed list of storage resources, assigning a unique index number to each LUN available. Specify the storage resources to map by using the appropriate index numbers.

Syntax

```
scsirouter name target name lun nn wwpn #?
scsirouter name target name lun nn {serial | lunwwn} #?
scsirouter name target name lun nn wwpn #nn [wwpn #nn]
scsirouter name target name lun nn {serial | lunwwn} #nn
scsirouter name target name wwpn #nn [wwpn #nn | wwpn
xx:xx:xx:xx:xx:xx:xx:xx]
```

Table 143: Syntax Description

<i>name (?)</i>	The name of the SCSI routing instance to which you are adding the storage target
<i>target name</i>	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid internal target name (ITN). There is a maximum of 100 targets per storage router or storage router cluster.
<i>lun nn</i>	The LUN number associated with the logical target. The LUN number is optional if mapping to a world-wide port number (WWPN) address type. The LUN number is required if mapping to a serial number or LUN world-wide name address type.
<i>#?</i>	The keyword used to request an indexed list of available storage resources on the Fibre Channel network
<i>serial</i>	Uses the serial number for the named storage resource
<i>wwpn</i>	Uses the world-wide port number (WWPN) address type for the named storage resource. You can specify a primary and optional secondary WWPN.

Table 143: Syntax Description (Continued)

<i>lunwwn</i>	Uses the LUN world-wide node name (LUNWWN) address type for the named storage resource
<i>#nn</i>	<p>The index number from the displayed list. The storage resource listed after the number specified is the physical storage address to which the logical target, or logical target and LUN combination, is to be mapped.</p> <p>When “#” is used with WWPN mapping this implies static FC port mapping. Meaning the FC port on the indexed line that is picked will be the only FC port used for the device. If dynamic FC port selection is desired for WWPN mapping do not use the “#” option just type in the WWPN.</p>
<i>wwpn</i> <i>xx:xx:xx:</i> <i>xx:xx:xx:</i> <i>xx:xx</i>	<p>Specifies a WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available. When this method is used the SR 2122 will be in dynamic FC port mode. Meaning it will determine the best path to use for the WWPN. (Optional)</p>

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter target {serial | lunwwn | wwpn}#?` command can be used for target-only or target and target-and-LUN mapping.

Part of the information included in the indexed list is the address type of each storage resource. The address type indicates what type of physical addressing can be used to access the storage resource: port ID, serial number, world-wide port number, or LUN world-wide name. If the list shows more than one address type for a storage resource, specify the address type you prefer for mapping to that storage resource.

To display the indexed list of storage resources, use the pound sign character (#) and the CLI list choices function (? key). This causes a list of devices discovered on the Fibre Channel network to display as a numbered (indexed) set of lines. The command is displayed below the list to the point of the # keyword. Complete the command by entering the appropriate index number.

When a target is added, it is enabled by default. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts or FC server instances. Use the `scsirouter target {enabled|disabled}` command to enable access to this storage target for selected IP hosts and FC servers.

To restore a previously configured target, use the complete internal target name (shown as the WWUI in the `show scsirouter` display) as the target name. The internal name is generated when a target is initially created.

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example displays an indexed list of storage resources available to SCSI routing instance *foo1* and maps the logical target *webserver8* to the WWPN represented by index number 2.

```
scsirouter foo1 target webserver8 wwpn #?
Fabric Attached Devices detected
Interface lunwwn          wwpn          portId  lun  vendor
product serial
-----
fc2          20000020371912cc 21000020371912cc 0x102e2 0   DEC
   HSG80    LS105203J6D
fc2          2000002037c52f42 2100002037c52f42 0x102e4 0   Compaq
MSA1000 3C8S700116D
fc2          2000002037c588d2 2100002037c588d2 0x102e8 0   DEC
   MSG80    3C56N20116D
fc2          2000002037c59d28 2100002037c59d28 0x102e1 0   DEC
   MSG80    3CC05V5Z06D
```

scsirouter target lun serial

To map a logical target and LUN combination to the product serial number of the physical storage resource, use the `scsirouter target lun serial` command. The `scsirouter target lun serial` command is a target-and-LUN mapping method of mapping a logical target and LUN combination to a physical storage resource by the LUN serial number.

Syntax

```
scsirouter name target name lun nn serial serial-text
```

Table 144: Syntax Description

<i>name (?)</i>	The name of the SCSI routing instance to which you are adding the storage target
<i>target name</i>	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid internal target name (ITN). There is a maximum of 100 targets per storage router or storage router cluster.
<i>lun nn</i>	The LUN number associated with the target (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255
<i>serial serial-text</i>	The product number of the physical LUN

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter target lun serial` command requires both a logical target and LUN combination, and the product serial number of the physical storage resource.

When a target is added, it is enabled by default. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts and FC server instances. Use the `scsirouter target {enabled | disabled}` command to enable access to this storage target for selected IP hosts and FC server instances.

To restore a configured target, use the complete internal target name (shown WWUI in the `show scsirouter display`) as the target name. The internal target name is generated when a target is initially created.

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example maps the logical target and LUN combination for SCSI routing instance *fool*. The logical target and LUN combination, *webserver9* LUN *1*, is mapped to the physical LUN with a serial number of *ST318451FC3CC05T3N00007116DLWQ*.

```
scsirouter fool target webserver9 lun 1 serial
ST3184551FC3CC05T3N0007116DLWQ
```

scsirouter target lun lunwwn

To map a logical target and LUN combination to a world-wide node name (LUNWWN) storage address, use the `scsirouter target lun lunwwn` command. The `scsirouter target lun lunwwn` command is a target-and-LUN mapping method of mapping a logical target to storage.

Syntax

```
scsirouter name target name lun nn lunwwn
xx:xx:xx:xx:xx:xx:xx:xx
```

Table 145: Syntax Description

<i>name (?)</i>	The name of the SCSI routing instance to which you are adding the storage target
<i>target name</i>	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid internal target name (ITN). There is a maximum of 100 targets per storage router or storage router cluster.
<i>lun nn</i>	The LUN number associated with the logical target. LUNs are integers between 0 and 255
<i>lunwwn</i> <i>xx:xx:xx:xx:xx:xx:xx:xx</i> <i>:xx:xx:xx</i>	The physical LUN world-wide name address. Note colons are optional

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter target lun lunwwn` command specifies a logical target name and LUN number combination to be mapped to a physical LUN world-wide name in storage.

Note: LUNWWN address notation is represented by 16 hex digits, usually formatted as eight pairs with each pair separated by a colon, xx:xx:xx:xx:xx:xx:xx:xx. When entering LUNWWN addresses, colons may be placed anywhere in the address notation, as long as they do not leave one character without a partner character. The entry should be zero-filled from the most significant (the left most) character position.

The following examples are **correct**:

- 0000:0000:1234:5678
- 0A0F2860:02111750

The following examples are **incorrect**:

- 1:234:567:8:91:23:FF:67
- 12:34:56

When a target is added, it is enabled by default. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts and FC server instances. Use the `scsirouter target {enabled | disabled}` command to enable access to this storage target for selected IP hosts and FC server instances.

To restore a previously configured target, use the complete internal target name (shown as the WWUI in the `show scsirouter display`) as the target name. The internal name is generated when a target is initially created.

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example maps a logical target and LUN combination for SCSI router services instance *foo1*. The logical target and LUN combination, *webserver5* LUN 5, is mapped to the physical LUNWWN *22:00:00:20:37:19:12:9d*.

```
scsirouter foo1 target webserver5 lun 5 lunwwn
22:00:00:20:37:19:12:9d
```

scsirouter target lun targetid

To map a logical target and LUN combination to a Parallel SCSI interface, use the `scsirouter target lun targetid` command.

Syntax

```
scsirouter name target name lun nn targetid #id
scsirouter name target name lun nn targetid id bus1 lun nn
scsirouter name target name lun nn targetid id bus2 lun nn
```

Table 146: Syntax Description

<i>name (?)</i>	The name of the SCSI routing instance to which you are adding the storage target
<i>#id</i>	Selects the target ID index. Use the #? to display the table mapping the index to a particular target ID
<i>target name</i>	A user-specified name of the logical target. There is a maximum of 100 targets per storage router or storage router cluster.
<i>lun nn</i>	The LUN number associated with the logical target. LUNs are integers between 0 and 255.
<i>targetid id</i>	The target ID number between 0 and 15
<i>bus1 lun nn</i>	The physical device LUN on Bus one interface
<i>bus2 lun nn</i>	The physical device LUN on Bus two interface

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter target lun targetid` command specifies a logical target name and LUN number combination to be mapped to a physical bus on the Parallel SCSI interface.

Examples

The following example maps a logical target and LUN combination for SCSI router services instance *foo1*. The logical target and LUN combination, *webserver5* LUN 5, is mapped to the physical lun 3 with targetid 4:

```
scsirouter foo1 target webserver5 lun 5 targetid 4 bus1 lun 3
```

scsirouter target lun wwpn lun

To map a logical target and LUN combination to a primary (and optional secondary) storage address where each storage address is specified by world-wide port name (WWPN) and LUN, use the `scsirouter target lun wwpn lun` command. The `scsirouter target lun wwpn lun` command is a target-and-LUN mapping method of mapping a logical target to storage.

Syntax

```
scsirouter name target name lun nn wwpn xx:xx:xx:xx:xx:xx:xx:xx
lun nn [wwpn xx:xx:xx:xx:xx:xx:xx:xx lun nn]
```

Table 147: Syntax Description

<i>name</i> (?)	The name of the SCSI routing instance to which you are adding the storage target
<i>target name</i>	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid internal target name (ITN). There is a maximum of 100 targets per storage router or storage router cluster.
<i>lun nn</i>	The first instance is the LUN number associated with the target (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255. The second instance is the LUN number associated with the primary WWPN (physical device LUN). Physical LUNs may be any physical device number, for example 0x51d1 or 123.
<i>wwpn</i> xx:xx:xx:xx:xx:xx:xx:xx	Specifies WWPN for the primary storage address
<i>wwpn</i> xx:xx:xx:xx:xx:xx:xx:xx xx:xx:xx:xx:xx:xx:xx:xx	Specifies WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available (Optional)
<i>lun nn</i>	Specifies the LUN associated with the optional secondary WWPN. Physical LUNs may be any physical device number, for example 0x51d1 or 123. (Optional)

Defaults

None.

Command Modes

Administrator

Usage Guidelines

The `scsirouter target lun wwpn lun` command specifies a logical target name and LUN number combination to be mapped to a physical WWPN and LUN combination in storage.

The secondary WWPN and LUN combination is optional. The secondary combination is mapped to the logical target name and LUN combination as an alternate, if the primary WWPN and LUN combination is not available.

When a target is added, it is enabled by default. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts and FC server instances. Use the `scsirouter target {enabled | disabled}` command to enable access to this storage target for selected IP hosts and FC server instances.

To restore a previously configured target, use the complete internal target name (shown as the WWUI in the `show scsirouter display`) as the target name. The internal name is generated when a target is initially created.

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of servers using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example maps a logical target and LUN combination for SCSI router services instance *foo1*. The logical target and LUN combination, *webserver7* LUN 7, is mapped to the primary WWPN and LUN combination, *22:00:00:20:37:19:15:05* LUN 0.

```
scsirouter foo1 target webserver7 lun 7 wwpn
22:00:00:20:37:19:15:05 lun 0
```

scsirouter target profile

To change the profile flag for a logical target, use the `scsirouter target profile` command. The `scsirouter target profile` command sets the profile of a target to either *high* or *low*, which turns ON/OFF some performance optimization for the target.

Syntax

```
scsirouter name target name profile high | low
```

Table 148: Syntax Description

<i>name</i> (?)	The name of the SCSI router instance to which you are adding the storage target
<i>target name</i>	The name of the logical target for which you want to change the profile
<i>profile</i> <i>low</i> <i>high</i>	Sets the target profile to either high (default) or low

Defaults

The default profile of a new created target is **high** profile.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter target profile` command sets a profile flag for a logical target. Setting a target profile to **high**, which is the default, enables performance enhancement features which may result in better I/O performance to that target. Setting a target profile to *low* optimizes for the memory usage in the system.

Examples

The following example sets the profile flag for target *webserver1* on the SCSI router instance *fool* to *low*:

```
scsirouter fool target webserver1 profile low
```

scsirouter target wwpn

To map a logical target to a primary (and, optionally, a secondary) storage address specified by world-wide port names (WWPNs), use the `scsirouter target wwpn` command. The `scsirouter target wwpn` command is a target-only method of mapping a logical target specified by WWPNs.

Syntax

```
scsirouter name target name wwpn xx:xx:xx:xx:xx:xx:xx:xx [wwpn  
xx:xx:xx:xx:xx:xx:xx:xx]
```

Table 149: Syntax Description

<i>name</i> (?)	The name of the SCSI routing instance to which you are adding the storage target
<i>target name</i>	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid internal target name (ITN). There is a maximum of 100 targets per storage router or storage router cluster.
<i>wwpn</i> xx:xx:xx:xx:xx:xx:xx:xx	Specifies a WWPN for the primary storage address
<i>wwpn</i> xx:xx:xx:xx:xx:xx:xx:xx xx:xx:xx	Specifies a WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter target wwpn` command requires only a logical target name to be mapped to a physical target address — no LUNS are specified. However, all LUNs that are part of the physical target address are discovered and made apparent as LUNs belonging to the logical target.

Note: WWPN address notation is represented by 16 hex digits, usually formatted as eight pairs with each pair separated by a colon, `xx:xx:xx:xx:xx:xx:xx:xx`. When entering WWPN addresses, colons can be placed anywhere in the address notation as long as they do not leave one character without a partner character. The entry should be zero-filled from the most significant (the left most) character position.

The following examples are **correct**:

- 0000:0000:1234:5678
- 0A0F2860:02111750

The following examples are **incorrect**:

- 1:234:567:8:91:23:FF:67
- 12:34:56

When a target is added, it is enabled by default . However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts and FC server instances. Use the `scsirouter target {enabled | disabled}` command to enable access to this storage target for selected IP hosts and FC server instances.

To restore a previously configured target, use the complete internal target name (shown as the WWUI in the `show scsirouter display`) as the target name. The internal name is generated when a target is initially created.

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example maps a logical target for SCSI router services instance *foo1*. The logical target *webserver1*, is mapped to the primary WWPN, *22:00:00:20:37:19:15:05*.

```
scsirouter foo1 target webserver1 wwpn 22:00:00:20:37:19:15:05
```

SCSI Router Commands

13

This section describes all the CLI commands related to the SCSI router feature in the system. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, history, usage guidelines, examples, and related commands.

accesslist

To create an access list entity, use the `accesslist` command.

Syntax

```
accesslist name
```

Table 150: Syntax Description

name	The name of the access list entity created by this command. Enter a maximum of 31 characters.
------	---

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Access lists specify the IP addresses of the IP hosts or FC server instances allowed to access common set of storage resources via the SR 2122 Storage Router. Access lists are associated with specific storage targets.

In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the `accesslist` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions.

Examples

The following command creates an access list named *webserver2*:

```
accesslist webserver2
```

```
accesslist <A.B.C.D/bits> | chap-username <userName> | iscsi-name  
<iscsiName>
```

To add the IP address and subnet mask of IP hosts and FC server instances to the named access list, use the `accesslist A.B.C.D/bits` command.

Syntax

```
accesslist name A.B.C.D/bits | A.B.C.D/1.2.3.4 [A.B.C.D/bits |  
A.B.C.D/1.2.3.4], . . . [A.B.D.F/bits | A.B.C.D/1.2.3.4]
```

To add a CHAP user name or an iSCSI host name to the named access list, use the `accesslist chap-username/iscsi-name` command.

```
accesslist name chap-username <chap-name>  
accesslist name iscsi-name <iscsi-name>
```

Table 151: Syntax Description

name (?)	The name of an access list to which you are adding information
A.B.C.D/bits	The IP address and subnet mask of the IP host or FC server instance being added to the access list. A.B.C.D is the dotted quad notation of the IP address. The /bits specifies the subnet mask in CIDR style.
A.B.C.D/ 1.2.3.4	The IP address and subnet mask of the IP host or FC server instance being added to the access list. A.B.C.D is the dotted quad notation of the IP address. 1.2.3.4 is the dotted quad notation of the subnet mask.
chap-username userName	The CHAP user name being added to the access list
iscsi-name iscsiName	The iSCSI name of the host to be added to the accesslist

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Access lists specify the host names, the Chap user names, and IP addresses of the IP hosts or FC server instances allowed to access a common set of storage resources via the SR 2122 Storage Router. The IP address of the FC server instance is the Gigabit Ethernet interface IP address configured for the instance. The iSCSI name is the unique name of the iSCSI initiator.

Use the `accesslist A.B.C.D/bits | chap-username | iscsi-name` command after creating an access list entity to populate the list.

Enter multiple addresses and masks, separating each by a space. Note that commas are no longer used to separate a list of arguments.

Note: In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the `accesslist A.B.C.D/bits` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions.

Examples

The following commands add the specified entries to the named access lists:

```
accesslist myAccessList 192.168.54.12/32 192.168.54.15/32
accesslist Webserver5 209.165.200.232/255.255.255.255
209.165.202.0/255.255.255.0
accesslist myAccessList1 chap-username myAuthorizedUserName
accesslist myAccessList2 iscsi-name myAuthorizediSCSIHostName
```

accesslist description

To add a description to an existing access list entity, use the `accesslist description` command.

Syntax

```
accesslist name description "text"
```

Table 152: Syntax Description

name (?)	The name of an existing access list entity
description text	The user-defined identification information associated with this access list. Enclose the description string in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Access lists specify the IP addresses of the IP hosts and FC server instances allowed to access a common set of storage resources via the SR 2122 Storage Router. Access lists are associated with specific storage targets.

In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the `accesslist` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions.

If the `accesslist` command is issued with the **description** keyword and the access list already exists, the description will be added to the existing access list entity.

An access list is not an "Access Control List" as in other products, but is rather a "Lun Access List" or "Host Permission List."

Examples

The following command adds a description to the access list named *webserver2*:

```
accesslist webserver2 description "Access list for company web
servers"
```

clear counters scsirouter

To reset various accumulated operational statistics for the specified SCSI routing instance, or all SCSI routing instances, use the `clear counters scsirouter` command.

Syntax

```
clear counters scsirouter {name / all} connection
clear counters scsirouter {name / all} host
clear counters scsirouter {name / all} target {name / all}
```

Table 153: Syntax Description

name (?)	Specifies the name of the SCSI routing instance for which counters will be cleared
all	The keyword used to clear counters for all SCSI routing instances
connection	The keyword used to clear operational statistics related to connections only
host	The keyword used to clear operational statistics related to currently connected hosts only
target name (?)	Clears operational statistics related to the specified target
target all	Clears operational statistics related to all targets

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

This command resets the specified operational statistics. It does not display the accumulated statistics before resetting the counters.

Examples

The following example clears the connection counters for the SCSI routing instance *myScsi1*. Clear various statistics if you want to troubleshoot a connection problem.

```
clear counters scsirouter myScsi1 connection
```

clear static

To clear the mapping of the IP host to Fibre Channel (FC) address for the specified World Wide Port Name (WWPN), use the **clear static** command. This command is only available when the storage router is deployed for static transparent SCSI routing.

```
clear static iscsibindings {all | xxxxxxxxxxxxxxxxxxxx}
```

Table 154: Syntax Description

iscsibindings all	Clear all IP host to FC address mappings.
iscsibindings xxxxxxxxxxxxxxxxxx x	Clear the mapping represented by this WWPN. WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When using WWPN addresses in this command, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character.

Default

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

User Guide Lines

When the storage router is deployed for static transparent SCSI routing, the IP host to FC address mappings are saved and retained in the storage router when it is restarted. If an IP host will no longer be accessing storage, or if you want the storage router to create a new mapping when the IP host logs in again, you can clear an existing mapping. Mappings can only be cleared if they are not currently in use.

To display the mappings that are currently configured in the storage router, use the **show static iscsibindings** command.

Examples

The following example displays the currently configured mappings, and then deletes the mapping for the IP host at IP address 10.1.20.2 (WWPN 280100065338d6c0):

```
[HP SR2122-2]# show static iscsibindings
Interface WWPN                Host IP Address  Host Name
-----
-----
fci1  280100065338d6c0 10.1.20.2      iscsi.cisco.testlab
fci1  280200065338d6c0 10.1.4.213
iqn.1987-05.com.cisco.02.0AB08...B6E5CCE.WIN1
fci2  290100065338d6c0 10.1.30.100    iqn.1987-05.com.cisco.02.
9FD389...36D3D3.NT10

[HP SR2122-2]# clear static iscsibindings 280100065338d6c0
Binding cleared for WWPN 280100065338d6c0
```

The following example clears all IP host to FC mappings saved in the storage router. If a mapping is in use by an IP host, the mapping will not be cleared.

```
[HP SR2122-2]# clear static iscsibindings all
```

Related Commands

Command	Description
<code>show static</code>	Display the currently configured IP host to FC address mappings saved in the storage router.
<code>static iscsibinding interface autolearn</code>	Enable and disable auto-learning of static WWPN bindings.
<code>static iscsibinding interface index</code>	Manually populate the iSCSI static binding table for the specified interface.

debug fcip

To enable trace facilities for debugging FCIP instances, use the **debug fcip** command. To disable debugging, use the **no** form of this command.

```
debug fcip name {mailboxtrace | packettrace mask}
no debug fcip name mailboxtrace
```

Table 155: Syntax Description

<code>name</code>	The name of the FCIP instance to be debugged.
<code>mailboxtrace</code>	Keyword, indicating that mail box tracing services will be enabled.
<code>packettrace mask</code>	Keyword, indicating that packet tracing services will be enabled. The mask value indicates the traces to capture, in hex. The default value, 0xFFFF, captures all traces. A value of 0x0000 turns off packet tracing.

Default

All trace facilities are enabled, by default. The packet trace mask value defaults to 0xFFFF, capturing all traces.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

The **debug fcip** command is designed for debug purposes, and should be used under the guidance of a Cisco Technical Support professional.

Use this command to trace traffic associated with the named FCIP instance. Use the **show debug fcip** command to view the trace buffer output. The *mask* value defaults to 0xFFF, all packets are traced. A *mask* value of 0x0000 will turn off packet tracing.

Debug settings are not persistent and will return to default value when the storage router is rebooted. To retain a mask value for packet tracing services, use the **fcip destination config** command with the **pkttracemask** keyword to change the FCIP instance configuration and then save the changes to the storage router bootable configuration.

Examples

The following example enables the debug mail box tracing services for the FCIP instance named *fcip1*:

```
[HP SR2122-2]# debug fcip fcip1 mailboxtrace
```

The following example enables the debug packet tracing services for the FCIP instance named *fcip2*. All packets will be traced.

```
[HP SR2122-2]# debug fcip fcip2 packettrace 0xffff
```

The following example disables debug mail box tracing services for the FCIP instance named *fcip1*:

```
[HP SR2122-2]# no debug fcip fcip1 mailboxtrace
```

The following example turns off all packet tracing services for the FCIP instance named *fcip2*:

```
[HP SR2122-2]# debug fcip fcip2 packettrace 0x0000
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>fcip destination config</code>	Configure operational parameters for the named FCIP instance.
<code>show debug fcip</code>	Display debugging information for the named FCIP instance.

debug scsirouter

To enable trace facilities for debugging SCSI routing instances, use the `debug scsirouter` command. To disable debugging, use the `no` form of this command.

Syntax

```
debug scsirouter name scsitrace
no debug scsirouter name scsitrace
```

Table 156: Syntax Description

<i>name (?)</i>	The name of the SCSI routing instance to be debugged
<i>scsitrace</i>	The keyword indicating tracing services will be enabled

Defaults

All trace facilities are disabled by default.

Command Modes

Administrator.

Usage Guidelines

When enabled at this level, debug tracing will trace traffic to and from all targets associated with the named SCSI routing instance. The logging level for the specified SCSI routing instance must be set to debugging. Change the logging

level for the console or the log file to *debugging* to capture the trace and debug message. Trace and debug messages are only written if the logging level is *debugging*.

Examples

The following example enables debug tracing facilities for a SCSI routing instance named *foo*:

```
debug scsirouter foo scsitrace
```

debug scsirouter target

To enable trace facilities for debugging a specific SCSI routing instance target and LUN combination, use the `debug scsirouter target` command. To disable debugging, use the `no` form of this command.

Syntax

```
debug scsirouter name target name lun nn scsitrace
no debug scsirouter name target name lun nn scsitrace
```

Table 157: Syntax Description

<i>name</i> (?)	The name of the SCSI routing instance to be debugged
<i>target name</i> (?)	The name of the target to be included in the trace
<i>lun nn</i>	The specific LUN associated with the target
<i>scsitrace</i>	The keyword indicating tracing services will be enabled

Defaults

All trace facilities are disabled by default.

Command Modes

Administrator.

Usage Guidelines

When enabled at this level, SCSI tracing will trace traffic to and from the specified target and LUN combination associated with the named SCSI routing instance. The logging level for the specified SCSI routing instance must be set to debugging. Change the logging level for the console or the log file to *debugging* to capture the trace and debug message. Trace and debug messages are only written if the logging level is *debugging*.

Examples

The following example enables SCSI tracing facilities for the target and LUN combination *myTarget*, LUN 0, associated with the SCSI routing instance named *foo*:

```
debug scsirouter foo target myTarget lun 0 scsitrace
```

delete accesslist

To delete an entire access list, all access lists, or a specified entry (IP address, chap-username, or iscsi-name) from the named access list, use the `delete accesslist` command. Deletions do not change the persistent storage router configuration until the relevant configuration information has been saved using the appropriate `save` command with the **bootconfig** keyword.

Syntax

```
delete accesslist all
delete accesslist name [all]
delete accesslist name [A.B.C.D/bits | A.B.C.D/1.2.3.4 ]
delete accesslist name chap-username userName
delete accesslist name iscsi-name iscsiName
```


Table 158: Syntax Description

name (?)	The name of the access list
A.B.C.D/ bits	The IP address and subnet mask of the IP host or FC server instance being deleted from the access list. A.B.C.D is the dotted quad notation of the IP address. The /bits specifies the subnet mask in CIDR style. Must specify at least one IP address with additional IP addresses separated by a space (Optional)
A.B.C.D/ 1.2.3.4	The IP address and subnet mask of the IP host or FC server instance being deleted from the access list. A.B.C.D is the dotted quad notation of the IP address. 1.2.3.4 is the dotted quad notation of the subnet mask. Must specify at least one IP address with additional IP addresses separated by a space (Optional)
chap- username <i>userName</i>	The CHAP user name being deleted from the access list (Optional)
iscsi-name <i>iscsiName</i>	The iSCSI name of the host being delete from the access list (Optional)
name all	Deletes all entries from the named access list
all	Deletes all access lists (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Because access lists are cluster entities, this operation affects all targets associated with this access list, regardless of where the associated SCSI routing instance is running within the SR 2122 cluster.

- Use the `delete accesslist name all` to clear all entries from the access list, but retain the access list entity.
- Use the `delete accesslist name` command with no additional parameters to completely delete the named access list.

Note: In a cluster environment, all access lists must be created and maintained on the first storage router to join the cluster. If you issue the `delete accesslist` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all access list functions.

Examples

The following example completely deletes the access list named *fooList* from the storage router's currently running configuration:

```
delete accesslist fooList
```

The following example deletes all entries from the access list named *fooList1*. The access list entity itself is not deleted from the storage router's currently running configuration:

```
delete accesslist fooList1 all
```

The following example deletes all access lists from the storage router's currently running configuration:

```
delete accesslist all
```

The following example deletes the specified IP address from the named access list, *fooList2*. This command does not update the storage router's bootable configuration until a `save accesslist bootconfig` or `save all bootconfig` command is issued:

```
delete fooList2 192.168.54.12/32
```

The following example deletes the specified CHAP username from the named access list, *fooList3*. This command does not update the storage router's bootable configuration until a `save accesslist bootconfig` or `save all bootconfig` command is issued:

```
delete fooList3 chap-username userName
```

The following example deletes the specified iSCSI host name from the named access list, *fooList4*. This command does not update the storage router's bootable configuration until a `save accesslist bootconfig` or `save all bootconfig` command is issued:

```
delete fooList4 iscsi-name iscsiName
```

delete fcip

To delete the named elements from the FCIP instance, or to delete the named instance or all FCIP instances, use the **delete fcip** command. This command does not change the persistent storage router configuration until the relevant configuration information has been saved using the appropriate **save** command with the **bootconfig** keyword.

Syntax

```
delete fcip {name | all}  
delete fcip name destination
```

Table 159: Syntax Description

name	The name of the FCIP instance.
all	Keyword, used to delete all FCIP instances from the storage router. You are not prompted to confirm your actions.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.
3.4.1	The destination <i>name</i> argument was removed.

Use this command if you want to reconfigure the FCIP instance. You can delete the peer destination or the entire FCIP instance, or all FCIP instances. You must save the configuration changes to update the storage router bootable configuration.

Examples

The following examples deletes the destination from the FCIP instance, *fcip2*:

```
[HP SR2122-2]# delete fcip fcip2 destination
```

The following example deletes all FCIP instances:

```
[HP SR2122-2]# delete fcip all
```

The following example deletes the FCIP instance named *fcip1*:

```
[HP SR2122-2]# delete fcip fcip1
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

delete scsirouter

To delete the named elements from the SCSI routing instance, use the `delete scsirouter` command. Deletions do not change the persistent storage router configuration until the relevant configuration information has been saved using the appropriate `save` command with the **bootconfig** keyword.

Syntax

```
delete scsirouter {all | name} connection nn
delete scsirouter {all | name} serverif ge? [vlan vid]
delete scsirouter {all | name} target {name | all} [lun nn]
delete scsirouter {all | name} target {name | all} [lun nn]
force
delete scsirouter {all | name} force
```

Table 160: Syntax Description

all	Deletes all SCSI routing instances from the storage router
name(?)	The name of the SCSI routing instance
connection nn	Deletes the specified connection from the named instance, or all instances. Use the show scsirouter command with the connection keyword to display connection IDs. (Optional)
force	The keyword that overrides normal protections, allowing the action to be performed (Optional)
lun nn	Deletes the specified iSCSI LUN from the named target or all targets (Optional)
serverif {ge?}	Deletes the interface for the named SCSI routing instance or all instances (Optional)
target name (?)	The name of the specified target to delete
target all	Deletes all targets from the named instance
vlan vid	Deletes the specified VLAN from the named SCSI routing instance or all instances (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

In a cluster environment, a storage router that is running a SCSI routing instance is known as the current primary for that instance. Under normal circumstances, changes to the SCSI routing instance can only be made on the storage router that is the current primary for that instance. The SCSI routing instance may be in a stopped state at the time it is deleted.

The **force** option overrides the normal protections that prevent the deletion of an instance from a storage router that is not the current primary for that instance. The **force** option should only be used when the storage router, or a specific SCSI routing instance, is in an abnormal state and cannot be recovered without rebooting.

When used with the target or LUN keywords, the **force** option allows the specified object to be deleted, even if in use by an iSCSI driver. Under normal circumstances, a target or LUN cannot be deleted if an iSCSI driver is logged in.

Note: When making changes to SCSI routing services (such as adding or deleting targets, or changing access) be sure to make the complimentary changes to the iSCSI driver configuration of servers using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers, readme and example configuration files from <http://www.hp.com>.

Examples

The following example deletes all targets associated with the SCSI routing instance named *foo*:

```
delete scsirouter foo target all
```

The following example deletes the specified VLAN from the Gigabit Ethernet interface used by the SCSI routing instance named *foo1*:

```
delete scsirouter foo1 serverif ge2 vlan 101
```

The following example deletes the entire SCSI routing instance named *foo3*:

```
delete scsirouter foo3
```

fcip

To create an FCIP instance, use the **fcip** command.

Syntax

`fcip name`

Table 161: Syntax Description

name	The name of the FCIP instance. Valid named are <i>fcip1</i> and <i>fcip2</i> .
------	--

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

FCIP provides connectivity between SANs. Technically, it employs Fibre Channel over TCP/IP (FCIP) to provide block oriented FC devices connectivity over an IP network. FCIP allows the interconnection of islands of FC storage area networks (SANs) over IP-based networks to form a unified SAN in a single FC fabric. The FCIP instance becomes a binding point for the association of other configuration parameters.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer HP SR2122-2 Storage Router or MDS 9000 Series system. Each FCIP instance requires one and only one peer.

There can be a maximum of 2 FCIP instances defined per storage router. Each FCIP instance is associated with:

- An internal FC interface *fci1* or *fci2* (*fci1* is initiator WWPNN1 and *fci2* is initiator WWPNN2). The FCIP instance named *fcip1* is associated with *fci1*; the instance named *fcip2* is associated with *fci2*. This association is made automatically.
- A network interface, which provides IP connectivity to the peer destination. The FCIP instance named *fcip1* uses the Gigabit Ethernet interface, *ge1*; the instance named *fcip2* uses *ge2*. If both Gigabit Ethernet interfaces are cabled to the same network, you can configure the FCIP instance to failover to the secondary interface in case of a failure on the primary interface.
- A destination, which is the IP address (or name) of the FCIP instance on the peer system. The destination configuration includes the connection protocol (TCP/IP) used between the FCIP instances.

This command updates the running configuration of the storage router. You must save the FCIP instance configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Issue the **save fcip** command with the **bootconfig** keyword to save the FCIP instance to the storage router bootable configuration.

Examples

The following example creates an FCIP instance named *fcip1*:

```
[HP SR2122-2]# fcip fcip1
```

Related Commands

Command	Description
<code>clear counters fcip</code>	Reset accumulated operational statistics for the specified SCSI routing instance.
<code>debug fcip</code>	Enable debugging for the named FCIP instance.
<code>delete fcip</code>	Delete the named FCIP instance or the specified element of the FCIP instance.
<code>fcip description</code>	Add user-defined identification information to the named FCIP instance.
<code>fcip destination config</code>	Configure operational parameters for the named FCIP instance.

<code>fcip destination tcpclient</code>	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance initiates the TCP connection.
<code>fcip destination tcpserver</code>	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance listens for the TCP connection from the named destination.
<code>fcip enable</code>	Stop or start the named FCIP instance.
<code>fcip networkif</code>	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
<code>restore fcip</code>	Restore the named FCIP instance from the named configuration file.
<code>save fcip</code>	Save configuration information for the named FCIP instance.
<code>show debug fcip</code>	Display debugging information for the named FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

fcip destination config

To configure operational parameters for the selected FCIP connection protocol type, use the **fcip destination config** command.

Syntax

```
fcip name destination config {rxtcpwinsize | txtcpwinsize} nn
fcip name destination config tcpport port-number
fcip name destination config batchtcp {yes | no}
fcip name destination config frinhiwater nn
fcip name destination config idlepingdelay nn
fcip name destination config compression {off | on}
fcip name destination config setPacing nnn
```

Table 162: Syntax Description

name	The name of this FCIP instance. Valid named are <i>fcip1</i> and <i>fcip2</i> .
rxtcpwinsize <i>nn</i>	The maximum number of outstanding bytes that can be received on a TCP connection. Valid values are 8192 to 2097152, inclusive. The default value is 262144. This configuration option applies to TCP client or TCP server connections only.
txtcpwinsize <i>nn</i>	The maximum number of outstanding bytes that can be transmitted on a TCP connection. Valid values are 8192 to 2097152, inclusive. The default value is 2097152. This configuration option applies to TCP client or TCP server connections only.
tcpport <i>port-number</i>	The TCP port number. The TCP server listens to this port; the TCP client connects to this port. Valid values are 0 to 65535, inclusive. The default port is 3225. This configuration option applies to TCP client or TCP server connections only.
batchtcp yes	Batch multiple FC frames in one TCP segment. This is the default. This configuration option applies to TCP client or TCP server connections only.
batchtcp no	Do not batch multiple FC frames in one TCP segment. Each FC frame is sent in a separate TCP segment. This configuration option applies to TCP client or TCP server connections only.
frinhiwater <i>nn</i>	The maximum number of frames, received from a raw IP connection, that can be sent to the Fibre Channel (FC) interface. Valid values are from 1 to 4294967294. The default value is 688. This configuration option applies to all FCIP connection types.
idlepingdelay <i>nn</i>	The number of seconds before a keep-alive packet is sent across an idle connection. Valid values are 1 to 65535, inclusive. The default value is 15. This configuration option applies to all FCIP connection types.

Table 162: Syntax Description (Continued)

<code>compression on</code>	Use compression on FCIP traffic to this destination. This configuration option applies to all FCIP connection types.
<code>compression off</code>	Do not use compression on FCIP traffic to and from this destination. This is the default. This configuration options applies to all FCIP connection types.
<code>setPacing nnn</code>	The value of the <code>setPacing</code> command can be from 0 to 999, with 0 as the default. This value indicates the bandwidth in Mbits/sec of the expected minimum bandwidth for this FCIP connection. Zero indicates full bandwidth of 1 Gigabit/sec.

The following are the default settings for all FCIP connection configuration options:

- TCP receive window size—262144 bytes
- TCP transmit window size—2097152 bytes
- TCP port number—3225
- Multiple FC frames are batched in one TCP segment.
- Maximum number of frames sent to FC interface—688 frames
- Maximum number of frames outstanding—1024 frames
- Maximum number of unacknowledged frames—16 frames
- Initial amount of delay before retransmission—0 ticks
- Maximum amount of time for retransmission—48 ticks
- Maximum amount of time a packet can be kept alive—0 ticks
- Value of IP protocol in IP header—4
- Maximum number of retransmissions—4
- The amount of time to increase the delay prior to retransmission—0 ticks
- The amount of time before a keep-alive ping is sent across an idle connection—15 seconds
- Packet trace mask—0xffff (packet tracing is enabled for all packets)
- The FCIP instance uses FC B_Port connectivity.
- FCIP compression is off.
- FCIP pacing default is set to 1 Gigabit/sec or off (o).

Note: One second is approximately 60 ticks.

Command modes

Administrator.

Command History

Command	Description
3.3.1	This command was introduced for the HP SR2122-2
3.4.1	The compression keyword was added and the destination <i>name</i> argument was removed.

Usage Guidelines

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer's protocol and IP address or name.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer HP SR2122-2 Storage Router or MDS 9000 Series system. Each FCIP instance requires only one peer. Both FCIP instances must be configured to use the same connection protocol, TCP/IP.

TCP/IP connection protocol uses the FCIP standard and TCP flow control and error recovery algorithms. FCIP, using TCP connections, allows you to configure TCP receive and transmit window sizes. Changes to TCP operational parameters are not applied until the FCIP instance is stopped and restarted, or the storage router is rebooted.

Examples

The following example add the destination at IP address *10.1.40.27* to the FCIP instance named *fcip1*. The FCIP instance is configured to use TCP/IP connection protocol and will initiate the connection (TCP client). The destinations TCP receive window size is set to 1 MB.

```
[HP SR2122-2]# fcip fcip1 destination tcpclient 10.1.40.27
*[HP SR2122-2]# fcip fcip1 destination config rxtcpwinsize 1048576
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>fcip destination tcpclient</code>	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance initiates the TCP connection.
<code>fcip destination tcpserver</code>	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance listens for the TCP connection from the named destination.
<code>fcip networkif</code>	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

fcip destination tcpclient

To add a peer destination to the named FCIP instance, with a connection type of TCP/IP, use the **fcip destination tcpclient** command. The named FCIP instance will initiate the TCP connection.

Syntax

```
fcip name destination tcpclient {A.B.C.D | servername}
```

Table 163: Syntax Description

name	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
A.B.C.D	The IP address of the peer destination. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The peer destination is the FCIP instance running in the partner storage router or MDS 9000 Series system
servername	The name of the peer system.

Command Modes

Administrator

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.
3.4.1	The destination <i>name</i> argument was removed and the <i>servername</i> argument was added.

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer's protocol and IP address or name.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer HP SR2122-2 Storage Router or MDS 9000 Series system. Each FCIP instance requires one and only one peer.

Use this command to configure a peer destination IP address (or name), using TCP/IP as the protocol type. When configured as a TCP client, the FCIP instance initiates the connection to the peer destination. The peer destination must be configured as a TCP server. The TCP server listens for the initial connection.

Note: The only functional difference between an FCIP instance configured as a TCP client and an FCIP instance configured as a TCP server is during the initial connection, which is initiated by the TCP client.

The destination IP address is the Gigabit Ethernet IP address of the FCIP instance running in the peer system.

TCP/IP connection protocol uses the FCIP standard and TCP flow control and error recovery algorithms. FCIP, using TCP connections, allows you to configure TCP receive and transmit window sizes.

Note: When configuring an FCIP instance, you must configure the network interface before you configure the peer destination and protocol.

Examples

The following example configures the FCIP instance named *fcip2* with a destination at IP address *10.1.4.32*, using TCP/IP connection protocol. The FCIP instance is configured as a TCP client, and will initiate the TCP connection to the destination.

```
[HP SR2122-2]# fcip fcip2 destination tcpclient 10.1.4.32
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>fcip destination config</code>	Configure operational parameters for the named FCIP instance.
<code>fcip networkif</code>	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

fcip destination tcpserver

To add a peer destination to the named FCIP instance, with a connection type of TCP/IP, use the **fcip destination tcpserver** command. The named FCIP instance will listen for the TCP connection from the named destination.

Syntax

```
fcip name destination tcpserver {A.B.C.D | servername}
```

Table 164: Syntax Description

name	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
A.B.C.D	The IP address of the peer destination. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The peer destination is the FCIP instance running in the partner storage router or MDS 9000 Series system.
servername	The name of the peer system.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.
3.4.1	The destination <i>name</i> argument was removed and the <i>servername</i> argument was added.

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer's protocol and IP address or name.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer HP SR2122-2 Storage Router or MDS 9000 Series system. Each FCIP instance requires one and only one peer.

Use this command to configure a peer destination IP address, using TCP/IP as the protocol type. When configured as a TCP server, the FCIP instance listens for the connection from the peer destination. The peer destination must be configured as a TCP client. The TCP client initiates the TCP initial TCP connection.

Note: The only functional difference between an FCIP instance configured as a TCP client and an FCIP instance configured as a TCP server is during the initial connection, which is initiated by the TCP client.

The destination IP address is the Gigabit Ethernet IP address of the FCIP instance running in the peer system.

TCP/IP connection protocol uses the FCIP standard and TCP flow control and error recovery algorithms. FCIP, using TCP connections, allows you to configure TCP receive and transmit window sizes.

Note: When configuring an FCIP instance, you must configure the network interface before you configure the peer destination and protocol.

Examples

The following example configures the FCIP instance named *fcip1* with a destination at IP address *10.1.5.222*, using TCP/IP connection protocol. The FCIP instance is configured as a TCP server, and will listen for the TCP connection from the destination.

```
[HP SR2122-2]# fcip fcip1 destination tcpserver 10.1.5.222
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>fcip destination config</code>	Configure operational parameters for the named FCIP instance.
<code>fcip networkif</code>	Assign a Gigabit Ethernet interface and IP address to the named FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

fcip enable

To start the named FCIP instance, use the **fcip enable** command. To stop the named FCIP instance, use the **no** form of this command.

Syntax

```
fcip {name | all} enable
no fcip {name | all} enable
```

Table 165: Syntax Description

name	The name of the FCIP instance to be started. Valid names are <i>fcip1</i> and <i>fcip2</i> .
all	Start all FCIP instances on this storage router.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

FCIP instances are automatically started by the storage router during the creation process and when the storage router is restarted. Use this command to manually control the running state of FCIP instances.

Use the **all** keyword to start all FCIP instances on the storage router. All instances previously stopped on this storage router will be restarted. This form of the command is always available; the only time the command is available for a named FCIP instance is when that FCIP instance has been previously stopped.

Examples

The following example starts the FCIP instance named *fcip2*. This instance must have been previously stopped.

```
[HP SR2122-2]# fcip fcip2 enable
```

The following example stops all FCIP instances running on the storage router:

```
[HP SR2122-2]# no fcip all enable
```

Related Commands

Command	Description
<code>delete fcip</code>	Delete the named FCIP instance or the specified element of the FCIP instance.
<code>fcip</code>	Create an FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

fcip networkif

To assign a Gigabit Ethernet interface and IP address to the named FCIP instance, use the **fcip networkif** command. The specified interface provides IP connectivity between the FCIP instance and its peer destination.

Syntax

```
fcip name networkif {A.B.C.D/bits | A.B.C.D/1.2.3.4}  
[secondary]
```

Table 166: Syntax Description

name	Name of the FCIP instance to which you are adding the Gigabit Ethernet interface. Valid names are <i>fcip1</i> and <i>fcip2</i> .
A.B.C.D/bits	The IP address of the named interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style. For the FCIP instance named <i>fcip1</i> , the IP address must be accessible from the Gigabit Ethernet interface, <i>ge1</i> . For the instance named <i>fcip2</i> , the IP address must be accessible from the interface <i>ge2</i> .
A.B.C.D/1.2.3.4	The IP address of the named interface. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.
secondary	(Optional) Indicates the specified IP address is available from both Gigabit Ethernet interfaces. If the primary interface goes down and remains down for two seconds, the specified IP address will be moved to the secondary interface.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

The specified interface IP address is configured as the destination IP address for the FCIP instance running in the peer system.

Each FCIP instance requires three active elements:

- The *networkif* element assigns an interface and IP address for use by the FCIP peer.
- The *destination* element assigns the peer's protocol and IP address or name.
- The device interface element associates the FCIP instance with an internal Fibre Channel interface and is automatically assigned and enabled.

An FCIP instance runs with a point-to-point connection to an FCIP instance on a peer HP SR2122-2 Storage Router or MDS 9000 Series system. Each FCIP instance requires one and only one peer.

Note: Each FCIP instance must connect to a unique peer system. If you have two FCIP instances running in a single storage router, you cannot connect both instances to the same peer system.

Use this command to configure an IP address for the FCIP instance, to be used by the FCIP peer for IP connectivity. For the FCIP instance named *fcip1*, the IP address is automatically associated with the Gigabit Ethernet interface, *ge1*. For the FCIP instance named *fcip2*, the IP address is automatically associated with the Gigabit Ethernet interface, *ge2*.

When configuring an FCIP instance, you must configure the network interface before you configure the peer destination and protocol.

If the **secondary** keyword is used, both Gigabit Ethernet interfaces must be connected to the same network segment. If the primary interface goes down and remains down for two seconds, the IP address will be moved to the secondary interface.

Note: If you configure a Gigabit Ethernet IP address with a secondary interface, all Gigabit Ethernet IP addresses on the same subnet must also be configured with the same secondary interface.

You can configure two FCIP instances on a single storage router to use the same network interface. You must fully configure one FCIP instance, and then configure a second FCIP instance without configuring a network interface. The second FCIP instance will use the same network interface as configured for the first instance. The two FCIP instances should use different connection protocols, or if both are configured as TCP servers, each FCIP instance must use a unique TCP port number.

Examples

The following command adds the IP address 10.1.10.128/24, to the FCIP instance named *fcip2*. This IP address will automatically be associated with the Gigabit Ethernet interface, *ge2*.

```
[HP SR2122-2]# fcip fcip2 networkif 10.1.10.128/24
```

The following command adds the IP address 10.1.30.128, with a netmask of 255.255.255.0, to the FCIP instance *fcip1*. This IP address is automatically associated with the Gigabit Ethernet interface, *ge1*. If the primary interface is not available, the IP address will be moved to the secondary Gigabit Ethernet interface, *ge2*. The Gigabit Ethernet interfaces must be connected to the same network.

```
[HP SR2122-2]# fcip fcip1 networkif 10.1.30.128/255.255.255.0  
secondary
```

The following set of commands configures the FCIP instance named *fcip1*, adds the network IP address 10.1.40.42/24, and configures the destination with a TCP client connection type. The second FCIP instance, *fcip2*, is configured with a destination and a TCP server connection type. Both FCIP instances will use the 10.1.40.42/24 network interface.

```
[HP SR2122-2]# fcip fcip1  
* [HP SR2122-2] fcip fcip1 networkif 10.1.40.42/24  
* [HP SR2122-2] fcip fcip1 destination tcpclient 10.1.1.144  
* [HP SR2122-2] fcip fcip2  
* [HP SR2122-2] fcip fcip2 destination tcpserver 10.1.5.73
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>fcip destination config</code>	Configure operational parameters for the named FCIP instance.
<code>fcip destination tcpclient</code>	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance initiates the TCP connection.
<code>fcip destination tcpserver</code>	Add a peer destination to the named FCIP instance, with a connection type of TCP/IP. The named FCIP instance listens for the TCP connection from the named destination.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

restore fcip

To cause the previously saved configuration information related to the named FCIP instance to be copied from the specified configuration file into the bootable configuration, use the **restore fcip** command. The configuration file must exist in the *savedconfig* directory. Use the **show savedconfig** command to display the contents of the *savedconfig* directory.

Note: This does not change the running configuration of the storage router.

Syntax

```
restore fcip {name | all} from filename
```

Table 167: Syntax Description

name	The name of the FCIP instance to be restored. Valid names are <i>fcip1</i> and <i>fcip2</i> .
all	Keyword to restore all FCIP instances.
from filename	The name of the configuration file containing the information to be restored. This file must exist in the <i>savedconfig</i> directory.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

The FCIP instance should be inactive before it is restored. Use the **no fcip enable** command to stop an active FCIP instance so it can be restored. After the specified FCIP instance is restored, it is automatically enabled and the running configuration of the storage router is updated.

A **restore** command never deletes existing FCIP instances. The **restore** command will add missing instances and will overwrite configuration information for existing instances of the same name. If necessary, you can delete the FCIP instance and then restore it from a saved configuration file.

Examples

The following example restores the FCIP instance *fcip1* from the configuration file named *fcip_backup001*:

```
[HP SR2122-2]# restore fcip fcip1 from fcip_backup001
```


Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>fcip enable</code>	Stop or start the named FCIP instance.
<code>save fcip</code>	Save configuration information for the named FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

save fcip

To save all configuration data associated with the named FCIP instance to nonvolatile memory, use the **save fcip** command.

Syntax

```
save fcip {name | all} {filename | bootconfig}
```

Table 168: Syntax Description

name	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
all	Save configuration data for all FCIP instances.
filename	The name of the file where the configuration data will be written. This file is stored in the <i>savedconfig</i> directory.
bootconfig	Save the FCIP instance from the running configuration to the bootable configuration, used when the storage router is restarted.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

You must save configuration data from the running configuration to the bootable configuration for it to be retained in the storage router when it is restarted. Configurations saved to a file can be moved between storage routers and can be restored at a later time.

Examples

The following example saves all FCIP instances currently running on this storage router to the bootable configuration, used when the storage router is restarted:

```
[HP SR2122-2]# save fcip all bootconfig
```

The following example saves the FCIP instance named *fcip1* to the file named *fcip_HP SR2122-2*:

```
[HP SR2122-2]# save fcip fcip1 fcip_HP SR2122-2
```

Related Commands

Command	Description
<code>fcip</code>	Create an FCIP instance.
<code>fcip enable</code>	Stop or start the named FCIP instance.
<code>restore fcip</code>	Restore the named SCSI routing instance from the named configuration file.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

scsirouter cdbretrycount

To specify the number of times a failed command should be retried before returning an error on the CDB, use the **scsirouter cdbretrycount** command.

Syntax

```
scsirouter name cdbretrycount nn
```

Table 169: Syntax Description

name	The name of this SCSI routing instance.
nn	The number of CDB retries. <i>nn</i> is an integer from 0 to 512. The default value is 6. There is one second between retries.

Defaults

The number of CDB retries is 6, by default.

Command Modes

Administrator.

Command History

Release	Modification
2.3.1	This command was introduced for the HP SR2122-2.
3.2.1	This command was introduced for the HP SR2122-2. For the HP SR2122-2, the default value was changed to 6 seconds.

Usage Guidelines

Use this command to change the number of times a failed CDB will be retried by the storage router before returning an error on the CDB. Retries occur every second. For example, with the default retry count value of 6, it would take 6 seconds before a failed command would be returned with an error.

If an intelligent storage array includes multiple paths between hosts and storage, lowering the CDB retry count value could change the triggering of failover situations.

Note: In a high availability cluster, the storage router may fail over a SCSI routing instance when some or all devices accessed through that instance cannot be reached, before the maximum number of CDB retries occurs.

Examples

The following example sets the CDB retry count value to 10:

```
[HP SR2122-2]# scsirouter transparent cdbretrycount 10
```

Related Commands

Commands	Description
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter

To create an instance of SCSI routing services, use the `scsirouter` command.

Syntax

```
scsirouter name
```

Table 170: Syntax Description

name	The name of the SCSI routing instance created by this command. Enter a maximum of 31 characters
------	---

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

SCSI routing is the routing of SCSI requests and responses between IP hosts and FC server instances in an IP network and storage devices in a storage network. The SCSI routing instance becomes a binding point for the association of other configuration parameters. A SCSI routing instance provides IP hosts and FC server instances access to storage devices.

There can be a maximum of 12 SCSI routing instances defined per storage router. If the storage router is a member of a cluster, no more than 12 instances can be defined across the cluster.

Examples

The following command create SCSI routing entity named *myCompanyWebserver2*.

```
scsirouter myCompanyWebserver2
```

scsirouter authentication

To change the authentication method list used by the iSCSI server to authenticate iSCSI clients, use the `scsirouter authentication` command.

Syntax

```
scsirouter name authentication option
```

Table 171: Syntax Description

<i>name</i>	The name of this SCSI routing instance
<i>authentication option</i>	The authentication method list used by the iSCSI server to authenticate iSCSI clients. The option is one of the authentication method lists configured through the <code>aaa authentication iscsi</code> command. See the documentation of "aaa" for more information on configuring a list of authentication methods.

Defaults

The default authentication is **None**.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter authentication` command allows you to change the method list used by the iSCSI server to authenticate iSCSI clients. Refer to the “aaa” documentation for more information on configuring authentication method lists.

Examples

The following example sets the authentication method used by the SCSI routing instance *fool* to “*none*”:

```
scsirouter fool authentication "none"
```

The following example sets the authentication method list used by the SCSI routing instance *fool* to the *default* method list:

```
scsirouter fool authentication "default"
```

scsirouter client authenticate

To enable AAA authentication for the named iSCSI client, use the `scsirouter client authenticate` command.

Syntax

```
scsirouter name client authenticate {yes | no}
```

Table 172: Syntax Description

<i>name</i>	The name of the SCSI routing services instance
<i>client</i>	The keyword used to indicate that the SCSI routing services instance is functioning as an iSCSI client
<i>authenticate</i>	The keyword indicating AAA authentication
<i>yes</i>	The keyword used to enable AAA authentication for the named iSCSI client
<i>no</i>	The keyword used to disable AAA authentication for the named iSCSI client

Defaults

AAA authentication is disabled.

Command Modes

Administrator.

Usage Guidelines

Servers using the named iSCSI client will use the AAA authentication method for access to storage devices via SCSI routing services on the storage router. Use the `aaa new-model` command to enable AAA authentication; use the `aaa authentication iscsi` command to configure the AAA authentication methods.

Examples

The following example enables AAA authentication for the iSCSI client named *Cfool*:

```
scsirouter Cfool client authenticate yes
```

scsirouter description

To add user-defined identification information to the named instance of SCSI routing instances, use the `scsirouter description` command.

Syntax

```
scsirouter name description "text"
```

Table 173: Syntax Description

<i>name</i>	The name of this SCSI routing instance
description "text"	User-defined identification information associated with this SCSI routing instance. If the string contains spaces, enclose it in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `scsirouter description` command allows you to add a new description or change an existing description. Descriptions are site specific.

Examples

The following example adds the description “Access to WebServer4 WebServer5” to the SCSI routing instance *foo1*:

```
scsirouter foo1 description "Access to Webservers4 Webservers5"
```

scsirouter enable

To start the named SCSI routing instance (or all instances) on this storage router, use the `scsirouter enable` command. To stop the named SCSI routing instance, or all instances, use the `no` form of this command.

Syntax

```
scsirouter {name | all} enable  
no scsirouter {name | all} enable
```

Table 174: Syntax Description

<i>name</i> (?)	The name of the SCSI routing instance to be started
<i>all</i>	Starts all SCSI routing instances on this storage router

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

SCSI routing instances that are in a stopped state are not running in the cluster. To restart a stopped SCSI routing instance, use the `scsirouter enable` command. Use the **all** keyword to start all instances on the storage router. All instances previously stopped on this storage router, or available instances not running elsewhere in the cluster, will start on this storage router.

Use the `scsirouter enable` command to bring a restored SCSI routing instance into the running configuration. A restored instance must be enabled before you can make any additional configuration changes to that instance.

Under normal circumstances, the SCSI routing instance can only be started from the storage router on which it was stopped.

Use the `scsirouter enable` command with no arguments or keywords to start all SCSI routing instances throughout the cluster.

SCSI routing instances are automatically started by the storage router when the Fibre Channel interface is added.

Examples

The following example starts all SCSI routing instances in the cluster:

```
scsirouter all enable
```

The following example starts the SCSI routing instance named `foo1`. This instance must have been previously stopped.

```
scsirouter foo1 enable
```

The following example stops all SCSI routing instances running on the storage router:

```
no scsirouter all enable  
scsirouter foo1 log critical
```

scsirouter failover

To build a list of storage routers to be used for failover purposes, use the **scsirouter failover** command.

Syntax

```
scsirouter name failover {primary | secondary} sysname
```

Table 175: Syntax Description

name	The name of the SCSI routing instance.
primary <i>sysname</i>	The name of the storage router in the cluster. In case of failure, the specified SCSI routing instance will be failed over to this storage router.
secondary <i>sysname</i>	(Optional) The name of the storage router in the cluster. If the primary storage router in the list cannot run the SCSI routing instance, it will be failed over to this storage router. Because a high availability cluster consists of two storage routers, this parameter is not used.

Defaults

None. By default, the HA failover list is not populated.

Command Mode

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122-2.
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

Use the **scsirouter failover** command to build a list of storage routers that will be used during the failover process. If the specified SCSI routing instance fails over, the cluster attempts to start running the instance on the storage router designated as the *primary* in the HA failover list. If that storage router cannot run the SCSI routing instance, the cluster will attempt to start the instance on the storage router designated as the *secondary* in the HA failover list.

If there is no primary or secondary storage router on the HA failover list when the SCSI routing instance fails over, the cluster uses normal failover algorithms to determine where the SCSI routing instance should run.

The storage routers specified as primary and secondary should be active in the cluster when the command is issued. If the specified storage router is not currently active in the cluster, the setting will not take effect until the node is added to the cluster and the SCSI routing instance is restarted.

Use the **clear scsirouter failover** command to remove the current primary or secondary storage router from the HA failover list.

Note: This command causes the SCSI routing instance configuration information to be saved and all nodes in the cluster to be updated.

Examples

The following example builds the HA failover list for the SCSI routing instance named *foo*. The primary storage router in the HA failover list is *HP SR2122-2*.

```
[HP SR2122-2]# scsirouter foo failover primary HP SR2122-2
```

Related Comments

Command	Description
<code>clear scsirouter failover</code>	Remove the designated primary or secondary storage router from the HA failover list for the specified SCSI routing instance.
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>failover scsirouter</code>	Cause the named SCSI routing instance to cease running on the storage router.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>scsirouter primary</code>	Identify a storage router as the preferred storage router to run the named SCSI routing instance.

Command	Description
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
setup scsi	Run the wizard to configure a SCSI routing instance.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter lun reset

To specify that “LUN reset” rather than “clear task” commands will be sent to the storage resources opened by the specified SCSI routing instance, use the **scsirouter lun reset** command.

Syntax

```
scsirouter name lun reset {yes | no}
```

Table 176: Syntax Description

name	The name of the SCSI routing instance. The specified SCSI routing instance must be running.
yes	Send “lun reset” to storage resources when they are opened.
no	Send “clear task” to storage resources when they are opened.

Defaults

The default is to send “clear task” commands to storage resources.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

It is preferable to send “LUN reset” commands if the device supports them. The specified SCSI routing instance must be running.

Examples

The following example enables “LUN resets” to all storage resources opened by the SCSI routing instance *foo2*:

```
[HP SR2122-2]# scsirouter foo2 lun reset yes
```

Related Commands

Command	Description
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>scsirouter primary</code>	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
<code>scsirouter serverif</code>	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter password

To assign a password to a SCSI routing instance for iSCSI authentication purposes, use the **scsirouter password** command.

Syntax

```
scsirouter name password {password-string | none}
```

Table 177: Syntax Description

name	The name of the SCSI routing instance.
password-string	The password associated with the named SCSI routing instance. If the password is encrypted (starts with "9"), enter a maximum of 170 characters. If the password is unencrypted (starts with "0"), enter a maximum of 66 characters. If the password is entered as an unencrypted text string, enter a maximum of 64 characters.
none	Keyword, removing any existing iSCSI password assigned to the named SCSI routing instance.

Defaults

None.

Command Modes

Administrator

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to assign a password to the SCSI routing instance for two-way iSCSI authentication. Two-way iSCSI authentication allows authentication of the IP host and also allows the IP host, acting as an iSCSI initiator, to require authentication of the SCSI routing instance, acting as an iSCSI target. The user name and password assigned to the SCSI routing instance are used by the IP host for iSCSI authentication purposes.

iSCSI authentication must be enabled for the named SCSI routing instance. If iSCSI authentication is not enabled, the user name and password assigned to the SCSI routing instance will not be used.

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are changed to “XXXXX” in the CLI command history cache, and are stored in the local username database in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.
- After initial entry, passwords display in their encrypted format. Use the **show scsirouter** command to display the SCSI routing instance authentication information. The following is an example display:

SCSI Router Authentication Information

Router	Authentication	Username	Password
zeus	web1	zeus_lab1	9
ea9bb0c57ca4806d3555f3f78a4204177a			

The initial “9” in the example display indicates that the password is encrypted.

- You can re-enter an encrypted password using the normal **scsirouter password** command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting password “9 ea9bb0c57ca4806d3555f3f78a4204177a” from the example above into the **scsirouter mars password** command would assign the SCSI routing instance *mars* the same iSCSI password as the SCSI routing instance *zeus*. This functionality allows passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password “0 123” for the SCSI routing instance *zeus*, enter this command:

```
scsirouter zeus password "0 0 123"
```

To enter the password “9 73Zjm 5” for SCSI routing instance *lab3*, use this command:

```
scsirouter lab3 password '0 9 73Zjm 5'
```


Examples

The following example enables iSCSI authentication, using the default authentication list, for the SCSI routing instance named *lab3* and assigns a user name of *lab3-admin* and a password of *testing* to the instance for two-way authentication:

```
[HP SR2122-2]# scsirouter lab3 authentication default
*[HP SR2122-2]# scsirouter lab3 username lab3-admin
*[HP SR2122-2]# scsirouter lab3 password testing
```

Related Commands

Command	Description
<code>scsirouter authentication</code>	Enable iSCSI authentication for the named SCSI routing instance.
<code>scsirouter username</code>	Assign a user name to a SCSI routing instance for iSCSI authentication purposes.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter primary

To assign the specified system as the preferred storage router for the named SCSI routing instance, use the **scsirouter primary** command.

Syntax

```
scsirouter name primary sysname
```

Table 178: Syntax Description

<code>name</code>	The name of this SCSI routing instance.
<code>primary sysname</code>	The system name of the preferred storage router.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
3.2.1	This command was introduced for the HP SR2122-2.

User Guidelines

At any given time, a SCSI routing instance can run on only one node in a cluster. If a SCSI routing instance has the **primary** attribute set, the specified storage router will take over running that instance upon system restart or whenever target and critical resources are available.

If the **primary** attribute is not set, the SCSI routing instance continues running on the node where it was started until it is explicitly stopped (via a **no scsirouter enable** command), it automatically fails over to another node in the cluster because targets or critical resources are unavailable, or an explicit **failover scsirouter** command is issued. This is the default behavior.

Use the **scsirouter primary** command if you always want the specified SCSI routing instance to run on a specific storage router in a cluster whenever that node is available (assuming target and critical resources are available). Use the **clear scsirouter primary** command to remove the currently configured primary value for the named SCSI routing instance.

Note: Setting the **primary** attribute saves the SCSI routing instance configuration and circulates those changes to the high availability cluster. If the specified storage router is available to the cluster and has all target and critical resources available, the SCSI routing instance will be immediately failed over. If the specified storage router is not available to the cluster, failover will occur as soon as that storage router becomes available to the cluster (assuming target and critical resources are available).

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about HA, cluster configuration, and managing SCSI routing instances in a cluster environment.

Examples

The following command designates the HP SR2122-2 *LabRouter1* as the storage router on which the SCSI routing instance named *foo* will always, under normal conditions, run.

```
[HP SR2122-2]# scsirouter foo primary LabRouter1
```

Related Commands

Command	Description
<code>clear scsirouter primary</code>	Remove the storage router configured as the primary for the named SCSI routing instance.
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>scsirouter failover</code>	Add the storage router to the HA failover list for the specified SCSI routing instance.
<code>scsirouter serverif</code>	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter serverif

To assign a Gigabit Ethernet interface and IP address to the named SCSI routing instance, use the **scsirouter serverif** command. The specified interface allows IP hosts access to Fibre Channel storage.

Syntax

```
scsirouter name serverif ge? {A.B.C.D/bits | A.B.C.D/1.2.3.4}
[secondary ge?]

scsirouter name serverif ge? vlan vid
{A.B.C.D/bits | A.B.C.D/1.2.3.4} [secondary ge?]
```

Table 179: Syntax Description

name	Name of the SCSI routing instance to which you are adding the Gigabit Ethernet interface.
serverif ge?	The name of the interface. When you type the scsirouter serverif command, followed by <i>?</i> , the CLI lists the interfaces available. You cannot specify a nonexistent interface.
A.B.C.D/bits	<p>The IP address of the named interface. If the keyword vlan is used, the IP address is part of the specified VLAN. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.</p> <hr/> <p>Note: The IP address must be on a unique subnet; you cannot configure an IP address that is on the same subnet as another storage router network interface.</p> <hr/>
A.B.C.D/1.2.3.4	<p>The IP address of the named interface. If the keyword vlan is used, the IP address is part of the specified VLAN. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.</p> <hr/> <p>Note: The IP address must be on a unique subnet; you cannot configure an IP address that is on the same subnet as another storage router network interface.</p> <hr/>
secondary ge?	(Optional) The name of the Gigabit Ethernet interface to be used as a secondary interface for the specified IP address. If the primary interface goes down and remains down for two seconds, the specified IP address will be moved to the secondary interface.
vlan vid	The keyword and the VLAN identifier.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
2.5.1	The secondary keyword was added.
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

The specified interface IP address is configured on IP hosts requiring access to storage resources through the storage router.

Each SCSI routing instance requires two active elements:

- The *serverif* element assigns an interface and IP address for use by IP hosts requiring access to storage resources. The instance becomes active when this interface is added. A SCSI routing instance can have multiple *serverif* elements; one IP address per logical interface can be configured for a SCSI routing instance.
- The *target* element is a complex item that specifies the mapping between LUNs on the storage devices and the host systems.

The **scsirouter serverif vlan** command is used to associate a VLAN with a SCSI routing instance. All traffic using the specified Gigabit Ethernet interface will be considered as part of the VLAN; all IP hosts accessing storage through the storage router using the specified Gigabit Ethernet interface IP address must connect as part of the specified VLAN.

When the SCSI routing instance is started, a logical interface (for example, ge2VLAN100) is created, which incorporates the physical interface and the VID. This logical interface can be displayed via the **show interface** command.

If the **secondary** keyword is used, both Gigabit Ethernet interfaces must be connected to the same network segment. If the primary interface goes down and remains down for two seconds, the IP address will be moved to the secondary interface.

Note: If you configure a Gigabit Ethernet IP address with a secondary interface, all Gigabit Ethernet IP addresses on the same subnet must also be configured with the same secondary interface.

Examples

The following command adds the Gigabit Ethernet interface *ge1*, with the IP address 10.1.10.128/24, to the SCSI routing instance named *foo2*.

```
[HP SR2122-2]# scsirouter foo2 serverif ge1 10.1.10.128/24
```

The following command adds the Gigabit Ethernet interface *ge2* and VLAN ID 45, with IP address 10.1.30.128/24, to the SCSI routing instance *fooA*. If the primary interface is not available, the IP address will be moved to the secondary Gigabit Ethernet interface, *ge1*. The Gigabit Ethernet interfaces must be connected to the same network.

```
[HP SR2122-2]# scsirouter fooA serverif ge2 vlan 45 10.1.30.128/24  
secondary ge1
```

Related Commands

Command	Description
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter slp enable

To enable the advertisement of the targets of the named SCSI routing instance with the Service Location Protocol (SLP) service, use the **scsirouter slp enable** command. To disable target advertisement, use the **no** form of this command.

Syntax

```
scsirouter name slp enable
no scsirouter name slp enable
```

Table 180: Syntax Description

name	Name of the SCSI routing instance. All targets associated with this SCSI routing instance are advertised with the SLP service.
------	--

Defaults

Advertising with the SLP Service is enabled for all targets.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

SLP is an IP protocol designed to make it easy for network clients to discover available services on a network and to learn about the configuration of those services. By default, SLP advertisement is enabled when:

- A SCSI routing instance is started by the storage router during the creation process.
- The storage router is restarted.
- A SCSI routing instance is failed over to another storage router in a cluster.

Use this command to manually disable and re-enable the advertisement of targets with the SLP service. When target advertisement is disabled, all existing targets for the specified SCSI routing instance are de-registered, and any new targets that are added will not be advertised.

Examples

The following example disables target advertisement for the SCSI routing instance named *foo* and deregisters all of its previously registered targets from the SLP service:

```
[HP SR2122-2]# no scsirouter foo slp enable
```

The following example re-enables target advertisement for the SCSI routing instance named *foo*:

```
[HP SR2122-2]# scsirouter foo slp enable
```


Related Commands

Command	Description
<code>show slp</code>	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
<code>slp findattr</code>	Discover the attributes of a specific SLP registered service.
<code>slp findsrvs</code>	Locate a SLP registered service of a specific type on the local subnet.
<code>slp findsrvtypes</code>	Discover all SLP registered service types on the local subnet.

scsirouter target accesslist

To associate the named access list with the specified target, use the **scsirouter target accesslist** command.

Syntax

```
scsirouter name target {name | all} accesslist
{name | any | none} [ro | rw]
```

Table 181: Syntax Description

<code>name</code>	The name of the SCSI routing instance to which this target belongs.
<code>target name</code>	The name of the storage target to associate with this access list. The target must already exist.
<code>target all</code>	Associate all targets with the named access list.
<code>accesslist name</code>	The name of the access list to associate with this storage target.
<code>accesslist any</code>	Allow connections and logins for the specified target from any IP host. This is effectively "open access."
<code>accesslist none</code>	Prevent any new connections or logins to this target from any IP hosts. This is effectively "no access."
<code>ro</code>	(Optional) Allow the IP hosts identified by the specified access list read-only device access.
<code>rw</code>	(Optional) Allow the IP hosts identified by the specified access list read/write device access. This is the default.

Defaults

If access type (read-only or read/write) is not specified, the default is read/write.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
3.2.1	This command was introduced for the HP SR2122-2. For the HP SR2122, the ro and rw keywords were added.

User Guidelines

An access list identifies the IP hosts allowed to access the associated storage target through the storage router. IP hosts can be identified by IP address, CHAP user name, or iSCSI Name. Access lists are associated with specific storage targets. Each target can be associated with one access list that provides IP hosts read/write device access and one access list that provides read-only device access.

When an IP host attempts to access a storage resource, the storage router first looks for a matching entry using the access list configured to allow read/write device access. If the IP host does not have a matching entry in the read/write access list, the access list configured for read-only device access (if any) is used. If the IP host does not have a matching entry on either access list, the IP host is denied access to the storage resource.

Note: Some host operating systems impose restrictions on the use of read-only access lists. For details, see the readme files and *Release Notes for Cisco iSCSI Driver* for your IP host operating system.

- Use the **target all** form of this command to create an association between the specified access list and all targets.
- Use the reserved access list name **none** to remove any access list associations for the specified target. This effectively prevents access to this storage target from any IP host.

- Use the reserved access list name **any** to allow access to this storage target from any IP host. This is effectively “open access.”
- Existing connections and logins are not affected by an access list change. However, if there are existing connections, the storage router issues a warning message with that information in response to this command.

Note: When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Examples

The following example creates an association between the storage target *webserver4* (accessed via SCSI routing instance *foo*) and the access list *webserver2*. By default, the IP hosts identified by the *webserver2* access list will be allowed read/write device access to the target.

```
[HP SR2122-2]# scsirouter foo target webserver4 accesslist  
webserver2
```

The following example provides the IP hosts identified in the access list named *media* read-only access to all targets accessed via SCSI routing instance *LabA*:

```
[HP SR2122-2]# scsirouter LabA target all accesslist media ro
```

Note: Some host operating systems impose restrictions on the use of read-only access lists. For details, see the readme files and *Release Notes for Cisco iSCSI Driver* for your IP host operating system.

The following example provides the IP hosts identified by the access list *webcheck* read-only device access, and provides the IP hosts identified by access list *webserver2* read/write device access, to the target *webserver3*:

```
[HP SR2122-2]# scsirouter foo target webserver3 accesslist webcheck
ro
Setting read-only accesslist to 'webcheck' for scsirouter 'foo'
target 'webserver3'
*[HP SR2122-2]# scsirouter foo target webserver3 accesslist
webserver2 rw
Setting read-write accesslist to 'webserver2' for scsirouter 'foo'
target 'webserver3'
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.

Command	Description
<code>scsirouter serverif</code>	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
<code>scsirouter target crc</code>	Control the usage of iSCSI cyclical redundancy check (CRC) on the specified target or all targets.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show accesslist</code>	Display the contents of the named access list or all access lists.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter target crc

To control the usage of iSCSI cyclical redundancy check (CRC) on the specified target or all targets, use the **scsirouter target crc** command.

Syntax

```
scsirouter name target {name | all} crc
{always | any | never | prefer-off | prefer-on}
```

Table 182: Syntax Description

<code>name</code>	The name of the SCSI routing instance to which this target belongs.
<code>target name</code>	The name of the storage target.
<code>target all</code>	Apply the specified iSCSI CRC usage to all targets associated with this SCSI routing instance.
<code>always</code>	Always force iSCSI CRC on the target.
<code>any</code>	The target supports both CRC and non-CRC modes. The use of CRC is negotiated to the initiator preference.

Table 182: Syntax Description (Continued)

never	The use of iSCSI CRC is disabled on this target.
prefer-off	The use of iSCSI CRC is not the preferred mode of operation for this target, but the target will negotiate the mode if CRC mode is the only mode supported by the initiator. This is the default setting.
prefer-on	The use of iSCSI CRC is the preferred mode of operation for this target, but the target will function in non-CRC mode if it is the only mode supported by the initiator.

Defaults

iSCSI CRC is not the preferred mode of operation for the target.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

CRC codes are shortened cyclic codes used for error detection. A target configured for iSCSI CRC as the preferred mode of operation (prefer-on) opts for data integrity over performance. A target configured for non-CRC mode as the preferred mode of operation (prefer-off) opts for performance over data integrity.

Depending on the initiator and target configurations, the usage of iSCSI CRC is negotiated. lists the CRC negotiation outcomes for each possible pair of CRC configurations.

Initiator CRC Mode	Target CRC Mode	CRC Negotiation Outcome
always	always	CRC is enabled.
	never	Negotiation is rejected. No session is established to the target.
	prefer-on	CRC is enabled.
	prefer-off	CRC is enabled.
	any	CRC is enabled.
never	always	Negotiation is rejected. No session is established to the target.
	never	CRC is disabled.
	prefer-on	CRC is disabled.
	prefer-off	CRC is disabled.
	any	CRC is disabled.
prefer-on	always	CRC is enabled.
	never	CRC is disabled.
	prefer-on	CRC is enabled.
	prefer-off	CRC is disabled.
	any	CRC is enabled.
prefer-off	always	CRC is enabled.
	never	CRC is disabled.
	prefer-on	CRC is enabled.
	prefer-off	CRC is disabled.
	any	CRC is disabled.

Examples

The following example configures the storage target *webserver4*, accessed through SCSI routing instanced *foo*, to always use iSCSI CRC:

```
[HP SR2122-2]# scsirouter foo target webserver4 crc always
```

The following example configures all storage targets accessed through SCSI routing instances *lab2*, to prefer the use of iSCSI CRC:

```
[HP SR2122-2]# scsirouter lab2 target all crc prefer-on
```

Related Commands

Command	Description
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter target accesslist</code>	Associate an access list with a specific SCSI routing instance target or all targets.
<code>scsirouter target enable</code>	Allow or disallow connections and logins for the named target.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter target description

To add a description to the named target, use the **scsirouter target description** command.

Syntax

```
scsirouter name target name description "user text"
```

Table 183: Syntax Description

<code>name</code>	The name of the SCSI routing instance to which this target belongs.
<code>target <i>name</i></code>	The name of the storage target.
<code>"<i>user text</i>"</code>	User-defined identification information associated with this storage target. If the description contains spaces, enclose the string in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

Target description information is an optional attribute of a SCSI routing instance. Use the **show scsirouter** command to display target description information.

Examples

The following example adds a description to the storage target *webserver4*, accessed through the SCSI routing instance *foo*:

```
[HP SR2122-2]# scsirouter foo target webserver4 description "Web
databases"
```

Related Commands

Command	Description
<code>accesslist</code>	Create an access list entity.
<code>accesslist A.B.C.D/bits</code>	Add IP addresses to an access list.
<code>accesslist chap-username</code>	Add CHAP user name entries to an access list.
<code>accesslist iscsi-name</code>	Add iSCSI Name entries to an access list.
<code>delete accesslist</code>	Delete a specific access list entry or an entire access list.
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore accesslist</code>	Restore the named access list or all access lists from the named configuration file.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.

Command	Description
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
setup scsi	Run the wizard to configure a SCSI routing instance.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target enable

To allow connections and logins for the named target, use the **scsirouter target enable** command. To disallow connections and logins for the named target, use the **no** form of this command.

Syntax

```
scsirouter name target {name | all} enable  
no scsirouter name target {name | all} enable [force]
```

Table 184: Syntax Description

name	The name of the SCSI routing instance to which this target belongs.
------	---

Table 184: Syntax Description (Continued)

<code>target name</code>	The name of the storage target.
<code>target all</code>	Allow connections for all targets of this SCSI routing instance to be enabled or disabled.
<code>force</code>	(Optional) Disable the target and forcibly remove any active iSCSI sessions.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
3.2.1	This command was introduced for the HP SR2122-2.
3.4.1	The force keyword was added.

Usage Guidelines

When you add a target to a SCSI routing instance, it is by default enabled. However, no access list is associated with the target, thus effectively preventing any access to the storage target from any IP hosts. When you associate an access list with a target, the specified connections and logins are allowed.

Use this command to control access without changing the target access list association.

Existing connections and logins are not affected by the **no** form of this command, but future connections and logins are not allowed. If existing IP hosts are connected, the storage router issues a warning message with that information in response to this command. Use the **force** keyword if you want to disable the target and forcibly remove any existing iSCSI sessions.

Use the reserved target name **all** to enable or disable connections for all targets of this SCSI routing instance.

Note: When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Examples

The following example enables connections for all targets of the SCSI routing instance *foo*.

```
[HP SR2122-2]# scsirouter foo target all enable
```

The following examples disables connections for the target *webservices2* of the SCSI routing instance named *lab2*:

```
[HP SR2122-2]# no scsirouter lab2 target webservices2 enable
```

Related Commands

Command	Description
<code>accesslist</code>	Create an access list entity.
<code>accesslist A.B.C.D/bits</code>	Add IP addresses to an access list.
<code>accesslist chap-username</code>	Add CHAP user name entries to an access list.
<code>accesslist iscsi-name</code>	Add iSCSI Name entries to an access list.
<code>delete accesslist</code>	Delete a specific access list entry or an entire access list.
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore accesslist</code>	Restore the named access list or all access lists from the named configuration file.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save accesslist</code>	Save configuration data for the named access list or all access lists.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>scsirouter primary</code>	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
<code>scsirouter serverif</code>	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
<code>scsirouter target accesslist</code>	Associate an access list with a specific SCSI routing instance target or all targets.
<code>scsirouter target maxcmdqueuedepth</code>	Specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show accesslist</code>	Display the contents of the named access list or all access lists.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter target {lunid | serial | wwpn} #?

To use an index method of mapping a logical target or a logical target and LUN combination to storage, use the **scsirouter target {serial | lunid | wwpn} #?** command. This command creates an indexed list of storage resources, assigning a unique index number to each LUN available. Specify the storage resources to map by using the appropriate index numbers.

Syntax

```
scsirouter name target name wwpn #?
scsirouter name target name [lun nn] wwpn #?
scsirouter name target name lun nn {serial | lunid} #?
scsirouter name target name wwpn #nn [wwpn #nn]
scsirouter name target name lun nn wwpn #nn [wwpn #nn] [force]
scsirouter name target name lun nn {serial | lunid} #nn [force]
```

Table 185: Syntax Description

name	Name of the SCSI routing instance to which you are adding the storage target.
target name	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high availability cluster.
lun nn	The LUN number associated with the logical target. The LUN number is optional if mapping to a World Wide Port Name (WWPN) address type. The LUN number is required if mapping to a serial number or LUN identifier.
#?	Request an indexed list of storage resources available on the Fibre Channel (FC) network.
serial	Use the serial number for the named storage resource. The storage resource must support unique serial numbers for each LUN.
wwpn	Use the World Wide Port Name (WWPN) address type for the named storage resource. You can specify a primary and optional secondary WWPN.

Table 185: Syntax Description (Continued)

lunid	Use the unique LUN identifier, assigned when the LUN is discovered by the FC interface.
#nn	The index number from the displayed list. The storage resource listed after the number specified is the physical storage address to which the logical target or logical target and LUN combination is to be mapped.
force	(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
2.5.1	The lunwwn keyword was replaced by the lunid keyword and the force keyword was added.
3.2.1	This command was introduced for the HP SR2122-2.

This command can be used for target-only or target-and-LUN mapping.

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first storage router in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second storage router in the cluster).

To display the indexed list of storage resources, use the number sign (#) character followed by a question mark (?). That action will cause a list of devices discovered on the FC network to display as a numbered (indexed) table. The original command is re-displayed at the prompt below the list to the point of the # keyword. Complete the command by entering the appropriate index number.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts. Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about configuring SCSI routing instances on the storage router.

Note: When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Use the **force** keyword to allow target-and-LUN mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example displays an indexed list of storage resources available to SCSI routing instance *lab2* and maps the logical target *webserver8* to the WWPN storage address represented by index number 2.

```
[HP SR2122-2]# scsirouter lab2 target webserver8 wwpn #?
```

				Device		
Id	I/F	WWPN	Lun	Type	Vendor	Product
1	fc1	2200001026448a0d	0	Disk	SEAGATE	ST217340FC
2	fc1	22000003be3203bc	0	Disk	SEAGATE	ST217341FC

```
*[HP SR2122-2]# scsirouter lab2 target webserver8 wwpn #2
```


Related Commands

Command	Description
<code>accesslist</code>	Create an access list entity.
<code>accesslist A.B.C.D/bits</code>	Add IP addresses to an access list.
<code>accesslist chap-username</code>	Add CHAP user name entries to an access list.
<code>accesslist iscsi-name</code>	Add iSCSI Name entries to an access list.
<code>delete accesslist</code>	Delete a specific access list entry or an entire access list.
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore accesslist</code>	Restore the named access list or all access lists from the named configuration file.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save accesslist</code>	Save configuration data for the named access list or all access lists.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>scsirouter primary</code>	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
<code>scsirouter serverif</code>	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
<code>scsirouter target accesslist</code>	Associate an access list with a specific SCSI routing instance target or all targets.
<code>scsirouter target enable</code>	Allow or disallow connections and logins for the named target.
<code>scsirouter target trespass</code>	Enable the active/passive controller trespass feature for the specified storage target.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show accesslist</code>	Display the contents of the named access list or all access lists.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter target lun lunid

To map a logical target and LUN combination to a unique LUN identifier, use the **scsirouter target lun lunid** command. The **scsirouter target lun lunid** command is a target-and-LUN mapping method of mapping a logical target to storage.

Syntax

```
scsirouter name target name lun nn lunid lun-identifier [force]
```

Table 186: Syntax Description

name	Name of the SCSI routing instance to which you are adding the storage target.
target name	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high availability cluster.
lun nn	The LUN number associated with the logical target. LUNs are integers between 0 and 255.
lunid lun-identifier	Use the unique LUN identifier, assigned when the LUN is discovered by the Fibre Channel interface. Enter either 16 or 32 hex digits.
force	(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
2.5.1	The force keyword was added.
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

The **scsirouter target lun lunid** command specifies a logical target name and LUN number combination to be mapped to a physical LUN by its unique LUN identifier. The LUN identifier is represented by 16 or 32 hex digits. The digits may be separated by colons.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about configuring SCSI routing instances on the storage router.

Note: When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Use the **force** keyword to allow mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example maps a logical target and LUN combination for SCSI router instance *foo*. The logical target and LUN combination, *webserver5* LUN 5, is mapped to the physical LUN represented by the LUN identifier *200000203719129d*.

```
[HP SR2122-2]# scsirouter foo target webserver5 lun 5 lunid
200000203719129d
```

Related Commands

Command	Description
<code>accesslist</code>	Create an access list entity.
<code>accesslist A.B.C.D/bits</code>	Add IP addresses to an access list.
<code>accesslist chap-username</code>	Add CHAP user name entries to an access list.
<code>accesslist iscsi-name</code>	Add iSCSI Name entries to an access list.
<code>delete accesslist</code>	Delete a specific access list entry or an entire access list.
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore accesslist</code>	Restore the named access list or all access lists from the named configuration file.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save accesslist</code>	Save configuration data for the named access list or all access lists.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>scsirouter primary</code>	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
<code>scsirouter serverif</code>	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
<code>scsirouter target accesslist</code>	Associate an access list with a specific SCSI routing instance target or all targets.

Command	Description
<code>scsirouter target enable</code>	Allow or disallow connections and logins for the named target.
<code>scsirouter target trespass</code>	Enable the active/passive controller trespass feature for the specified storage target.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show accesslist</code>	Display the contents of the named access list or all access lists.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter target lun serial

To map a logical target and LUN combination to the serial number of the physical LUN, use the **scsirouter target lun serial** command. The **scsirouter target lun serial** command is a target-and-LUN mapping method of mapping a logical target and LUN combination to a physical storage resource by the LUN serial number.

Syntax

```
scsirouter name target name lun nn serial serial_number [force]
```

Table 187: Syntax Description

<i>name</i>	Name of the SCSI routing instance to which you are adding the storage target.
<i>target name</i>	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high availability cluster.
<i>lun nn</i>	The LUN number associated with the target (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255.
<i>serial serial_number</i>	The serial number of the physical LUN. The storage resource must support unique serial numbers for each LUN.
<i>force</i>	(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
2.5.1	The force keyword was added.
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

The **scsirouter target lun serial** command requires both a logical target and LUN combination and the serial number of the physical LUN.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about configuring SCSI routing instances on the storage router.

Note: When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

- Use the **force** keyword to allow mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example maps the logical target and LUN combination for SCSI routing instance *lab2*. The logical target and LUN combination, *webserver9* LUN *1*, is mapped to the physical LUN with a serial number of *ST318451FC3CC05T3N00007116DLWQ*.

```
[HP SR2122-2]# scsirouter lab2 target webserver9 lun 1 serial
ST318451FC3CC05T3N00007116DLWQ
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
delete scsirouter	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
restore scsirouter	Restore the named SCSI routing instance from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
save scsirouter	Save configuration information for the named SCSI routing instance.
scsirouter	Create a SCSI routing instance.
scsirouter enable	Stop or start the named SCSI routing instance.
scsirouter primary	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
scsirouter serverif	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.

Command	Description
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
scsirouter target enable	Allow or disallow connections and logins for the named target.
setup scsi	Run the wizard to configure a SCSI routing instance.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

scsirouter target lun wwpn lun

To map a logical target and LUN combination to a primary (and optional secondary) storage address where each storage address is specified by World Wide Port Name (WWPN) and LUN, use the **scsirouter target lun wwpn lun** command. The **scsirouter target lun wwpn lun** command is a target-and-LUN mapping method of mapping a logical target to storage.

Syntax

```
scsirouter name target name lun nn wwpn xxxxxxxxxxxxxxxx lun nn  
[wwpn xxxxxxxxxxxxxxxx lun nn] [force]
```

Table 188: Syntax Description

name	Name of the SCSI routing instance to which you are adding the storage target.
target name	A user-specified name of the logical target. Enter a maximum of 31 characters or a valid iSCSI Name. There is a maximum of 100 targets per storage router or per high-availability cluster.
lun nn	The first instance is the LUN number associated with the target (the iSCSI LUN). iSCSI LUNs are integers between 0 and 255. The second instance is the LUN number associated with the primary WWPN (physical device LUN). Physical LUNs may be any physical device number, for example 0x51d1 or 123.

Table 188: Syntax Description (Continued)

<code>wwpn xxxxxxxxxxxxxxxxxxxx</code>	Specify a WWPN for the primary storage address. In a high availability cluster, this is the WWPN for the storage resource as known to the first storage router in the cluster.
<code>wwpn xxxxxxxxxxxxxxxxxxxx</code>	(Optional) Specify a WWPN for the secondary storage address, used as an alternate for mapping if the primary is not available. In a high availability cluster, this is the WWPN for the storage resource as known to the second storage router in the cluster.
<code>lun nn</code>	(Optional) Specify the LUN associated with the optional secondary WWPN. Physical LUNs may be any physical device number, for example 0x51d1 or 123.
<code>force</code>	(Optional) Keyword used to allow LUN-mapping of the same storage array control LUNs in multiple targets.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the HP SR2122.
2.5.1	The force keyword was added.
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guideline

The **scsirouter target lun wwpn lun** command specifies a logical target name and LUN number combination to be mapped to a physical WWPN and LUN combination in storage.

Tips

WWPN address notation is represented by 16 hex digits. The digits may be separated by colons. When entering WWPN addresses, colons can be omitted or placed anywhere in the address notation as long as they do not leave one character without a partner character. The entry should be zero-filled from the most significant (the left-most) character position.

The following examples are *correct*:

- 0000:0000:1234:5678
- 0A0F2860:02111750
- 0A0F286002111750

The following examples are *incorrect*:

- 1:234:567:8:91:23:FF:6
- 12:34:56

The secondary WWPN and LUN combination is optional. The secondary combination is mapped to the logical target name and LUN combination as an alternate, if the primary WWPN and LUN combination is not available.

When you map a target using WWPN and the target needs to be accessed in a high availability cluster, you must specify both the primary WWPN (the WWPN of the storage resource as known to the first storage router in the cluster) and the secondary WWPN (the WWPN of the storage resource as known to the second storage router in the cluster). The secondary WWPN value may need to be retrieved by issuing the appropriate commands (such as the **show devices** command) from the second node in the cluster, or by temporarily attaching the secondary port of the storage device to the first storage router.

When a target is added, it is by default enabled. However, it is not associated with any access list (“accesslist none”), effectively disabling access to the target from any IP hosts. Use the **scsirouter target accesslist** command to enable access to this storage target for selected IP hosts.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about configuring SCSI routing instances on the storage router.

Note: When making changes to SCSI routing instances (such as adding or deleting targets or changing access) be sure to make the complimentary changes to the iSCSI configuration of IP hosts using these services to access the storage resources. See the readme files for the appropriate iSCSI drivers for additional details. You can access the latest iSCSI drivers and readme and example configuration files from Cisco.com.

Use the **force** keyword to allow mapping of the same storage array control LUN in multiple targets. Do not use the **force** keyword to LUN-map the same data LUN in multiple targets. LUN-mapping of the same LUN in multiple targets is advised for a control LUN on a storage controller only.

Examples

The following example maps a logical target and LUN combination for SCSI router instance *lab3*. The logical target and LUN combination, *webserver7* LUN 7, is mapped to the primary WWPN and LUN combination, *2200002037191505* LUN 0.

```
[HP SR2122-2]# scsirouter lab3 target webserver7 lun 7 wwpn
2200002037191505 lun 0
```

The following example maps a logical target and LUN combination to a primary and secondary WWPN. You may need to obtain the secondary WWPN from the storage router to which the secondary port of the device is attached, or temporarily attach the storage device's secondary port to the storage router being configured.

```
[HP SR2122-2]# scsirouter lab4 target webserver8 lun 0 wwpn
2200002037c6756d lun 0 wwpn 2100002037c6747f lun 0
```

Related Commands

Command	Description
<code>accesslist</code>	Create an access list entity.
<code>accesslist A.B.C.D/bits</code>	Add IP addresses to an access list.
<code>accesslist chap-username</code>	Add CHAP user name entries to an access list.
<code>accesslist iscsi-name</code>	Add iSCSI Name entries to an access list.
<code>delete accesslist</code>	Delete a specific access list entry or an entire access list.

Command	Description
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore accesslist</code>	Restore the named access list or all access lists from the named configuration file.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save accesslist</code>	Save configuration data for the named access list or all access lists.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>scsirouter primary</code>	Identify a storage router as the preferred storage router to run the named SCSI routing instance.
<code>scsirouter serverif</code>	Assign a Gigabit Ethernet interface, IP address, and optionally a VLAN to the named SCSI routing instance.
<code>scsirouter target accesslist</code>	Associate an access list with a specific SCSI routing instance target or all targets.
<code>scsirouter target enable</code>	Allow or disallow connections and logins for the named target.
<code>scsirouter target trespass</code>	Enable the active/passive controller trespass feature for the specified storage target.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>show accesslist</code>	Display the contents of the named access list or all access lists.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter target maxcmdqueuedepth

To specify the maximum number of commands allowed at any given time from each iSCSI session to the specified target, use the **scsirouter target maxcmdqueuedepth** command.

Syntax

```
scsirouter name target {all | name} maxcmdqueuedepth nn
```

Table 189: Syntax Description

name	Name of the SCSI routing instance.
target all	Specify the maximum number of command for all targets.
target name	The name of the storage target.
nn	The maximum number of commands allowed from each iSCSI session. If the value is set to zero, the feature is disabled.

Defaults

This feature is disabled; **maxcmdqueuedepth** is set to zero.

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced.

Usage Guidelines

When this value is configured, all current and future iSCSI sessions to the specified target will enforce the maximum command queue depth. To disable this feature, and allow an unlimited number of commands to the target from each iSCSI session, set the **maxcmdqueuedepth** to zero. This is the default setting.

Use the **show scsirouter** command with the **bootconfig** or **runningconfig** keyword to display the current maximum command queue depth value.

Note: Normal limitations, based on the available command buffer space, are always enforced. Setting the maximum command queue depth does not override these normal limitations.

Examples

The following example sets the maximum command queue depth to 20, for all targets associated with the SCSI routing instance named *foo*.

```
[HP SR2122-2]# scsirouter foo target all maxcmdqueuedepth 20
```

The following example disables the maximum command queue depth, allowing an unlimited number of commands to the target named *webservices2*, associated with the SCSI routing instance named *foo*.

```
[HP SR2122-2]# scsirouter foo target webservices2 maxcmdqueuedepth 0
```

scsirouter target trespass

To enable the active/passive controller trespass feature for the specified storage target, use the **scsirouter target trespass** command. To disable the trespass feature, use the **no** form of this command.

Syntax

```
scsirouter name target {all | name} trespass
no scsirouter name target {all | name} trespass
```

Table 190: Syntax Description

name	Name of the SCSI routing instance to which you are adding the trespass feature.
target all	Enable the trespass feature for all targets.
target name	The name of the storage target.

Defaults

The trespass feature is disabled for all targets.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced.

Usage Guidelines

The trespass feature provides LUN failover capability for selected storage arrays that operate on the active/passive port model. When enabled, the trespass feature provides a redundant path from the storage router to the storage array by allowing the storage router to detect a path failure to a storage array port and perform the necessary operations to fail LUNs over to the other port on the storage array without using any multi-path software.

The trespass feature requires the SCSI routing instance target to be LUN mapped, using primary and secondary WWPNs, or LUN mapped using LUN ID. The proper mapping, along with the activation of the trespass feature, ensures that the storage router will detect a path failure and fail the LUNs over to the other port on the storage array.

This feature also provides redundant paths from the storage router to the storage array, and can be used in a high availability cluster.

Note: After enabling the trespass feature, restart the SCSI routing instance to activate the feature.

Examples

The following example enables the trespass feature for the target *labserver7*, associated with SCSI routing instance *lab3*. The SCSI routing instance is then disabled and reenabled to activate the trespass feature.

```
[HP SR2122-2]# scsirouter lab3 target labserver7 trespass
*[HP SR2122-2]# no scsirouter lab3 enable
*[HP SR2122-2]# scsirouter lab3 enable
```

Related Commands

Command	Description
<code>delete scsirouter</code>	Delete the named SCSI routing instance or the specified element of the SCSI routing instance.
<code>restore scsirouter</code>	Restore the named SCSI routing instance from the named configuration file.
<code>save scsirouter</code>	Save configuration information for the named SCSI routing instance.
<code>scsirouter</code>	Create a SCSI routing instance.
<code>scsirouter enable</code>	Stop or start the named SCSI routing instance.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

scsirouter username

To assign a user name to a SCSI routing instance for iSCSI authentication purposes, use the **scsirouter username** command.

Syntax

```
scsirouter name username {user-name | none}
```

Table 191: Syntax Description

<code>name</code>	The name of the SCSI routing instance.
<code>user-name</code>	A valid user name. Enter a maximum of 63 characters
<code>none</code>	Keyword, removing any existing iSCSI user name assigned to the named SCSI routing instance.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to assign a user name to the SCSI routing instance for two-way iSCSI authentication. Two way iSCSI authentication allows authentication of the IP host and also allows the IP host, acting as an iSCSI initiator, to require authentication of the SCSI routing instance, acting as an iSCSI target. The user name and password assigned to the SCSI routing instance are used by the IP host for iSCSI authentication purposes.

iSCSI authentication must be enabled for the named SCSI routing instance. If iSCSI authentication is not enabled, the user name and password assigned to the SCSI routing instance will not be used.

Examples

The following example enables iSCSI authentication, using the default authentication list, for the SCSI routing instance named *lab3* and assigns a user name of *lab3-admin* and a password of *testing* to the instance for two-way authentication:

```
[HP SR2122-2]# scsirouter lab3 authentication default
*[HP SR2122-2]# scsirouter lab3 username lab3-admin
*[HP SR2122-2]# scsirouter lab3 password testing
```

Related Commands

Command	Description
<code>scsirouter authentication</code>	Enable iSCSI authentication for the named SCSI routing instance.
<code>scsirouter password</code>	Assign a password to a SCSI routing instance for iSCSI authentication purposes.
<code>show scsirouter</code>	Display configuration and operational information for the named SCSI routing instance.

setup fcip

To configure an FCIP instance, use the **setup fcip** configuration wizard. The wizard prompts you to choose the name of the FCIP instance and specify the Gigabit Ethernet IP address and network mask. Then the wizard prompts you to enter the peer IP address and the connection protocol type. More extensive configuration of FCIP instances can be performed via the CLI or the web-based GUI.

Syntax

```
setup fcip [parameter1 parameter2...]
```

Table 192: Syntax Description

<code>parameter1</code> <code>parameter2 ...</code>	(Optional) Enter each parameter that the wizard prompts for. All parameters must be passed. If a parameter includes an embedded space, enclose the parameter in quotation marks.
--	--

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current default FCIP instance name is *fcip1*.

```
Create which FCIP instance ? [fcip1/fcip2 (fcip1)]
```

Command Modes

Administrator.

Command History

Release	Modification
3.3.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

The **setup fcip** command can only be run when at least one FCIP instance is not currently configured on the storage router; if both FCIP instances are configured, you cannot run the **setup fcip** wizard. Only one setup wizard can be active at any given time. Multiple users cannot run multiple setup wizards concurrently.

- Use the optional *parameter* arguments to run the **setup fcip** wizard from a command script. All parameters required by the wizard must be included. The **setup fcip** wizard will not complete unless all parameters are passed.

Note: If too many parameters are passed, the **setup fcip** wizard will ignore the extra parameters and may complete. If a parameter is not in the correct format or is otherwise invalid, the next parameter is used to attempt to fulfill the prompt. In either case, unexpected results could occur. Always check the output from a **setup fcip** command when using the *parameter* arguments.

Examples

The following shows example output and input for the **setup scsi** command:

```
[techpubs4]# setup fcip
```

In order to correctly configure this FCIP instance, be sure you know the configuration of the remote FCIP instance. You will need to know the IP address and the communication protocol of the remote FCIP instance. In addition, you will need to ensure that the Fibre Channel domain ID you assign is different than the Fibre Channel domain ID assigned to the remote HP SR2122-2.

The system enables you to create two FCIP instances. Each instance uses a different Fibre Channel interface and gigabit Ethernet interface.

```
Create which FCIP instance ? [fcip1/fcip2 (fcip1)] fcip2
Please specify an IP address and netmask for the gigabit Ethernet
interface. IP address? [A.B.C.D/nn] 10.1.0.16/24
```

If both gigabit Ethernet interfaces are cabled to the same network, you can configure the FCIP instance to failover to the secondary interface in case of a failure on the primary interface.

Configure secondary interface for the FCIP instance? [yes/no (no)]

no

Please enter the IP address of the remote FCIP instance to which you wish to connect.

IP address of remote FCIP instance? [A.B.C.D] **10.1.0.47**

Choose how you want the FCIP instance to communicate with the remote FCIP instance. If the remote FCIP instance is configured as a TCP server, select client. If the remote FCIP instance is configured as a TCP client, select server.

Use which protocol? [client/server] **client**

If this is the first FCIP instance to be configured on the storage router, you will be prompted to specify a Fibre Channel domain ID:

Please specify a domain ID for use by this FCIP instance. This domain ID must be unique.

It can not be assigned to any switch in the Fibre Channel fabric that this switch is connected to or assigned to any switch in the remote Fibre Channel network.

Domain ID for the Fibre Channel switch? [1 - 127] **80**

set Domain ID on Fibre Channel interfaces to 80

Mar 14 15:08:48: %FC-5-FCIP09: fcip2 has been started

FCIP, fcip2, created Mar 14 15:08:48: %UI-5-FAFD2: Added FCIP device fci2

Mar 14 15:08:48: %UI-5-NMAOOI: Address 10.1.0.16/24 is now operational on interface ge1

Mar 14 15:08:48: %UI-5-FAFNI: Added FCIP network interface ge2, 10.1.0.16/255.255.255.0

FCIP-2: addPeer server 10.1.0.47

Mar 14 15:08:48: %UI-5-FAFD: Added FCIP destination dest2 (server, 10.1.50.50)

Configuration complete.

FCIP instance fcip2 is now configured.

Done with setup.

Note: This process must be repeated for both the client and the server sides of the SR 2122-2.

Related Commands

Command	Description
<code>clear conf</code>	Return most configuration settings to factory defaults.
<code>setup</code>	Run the setup configuration wizard.
<code>setup access</code>	Run the wizard to configure Monitor mode and Administrator mode passwords.
<code>setup cluster</code>	Change the configuration of the high availability environment.
<code>setup iscsi-port</code>	Run the wizard to manually configure the port used for iSCSI traffic.
<code>setup mgmt</code>	Run the wizard to configure the management interface.
<code>setup netmgmt</code>	Run the wizard to configure network management.
<code>setup scsi</code>	Run the wizard to configure a SCSI routing instance.
<code>setup time</code>	Run the wizard to configure the system date and time.

show accesslist

To display a list of access lists or the contents of the named access list (or all access lists), use the `show accesslist` command.

Syntax

```
show accesslist [name | all]
show accesslist [name | all] from {bootconfig | file |
runningconfig}
```

Table 193: Syntax Description

name (?)	The name of the access list (Optional)
all	The keyword used to display all access list entries (Optional)
from bootconfig	The keywords used to display the access list information from the persistent saved configuration (Optional)
from file	The name of the configuration file where the access list configuration is stored. This file must exist in the savedconfig directory (Optional)
from runningconfig	The keywords used to display the access list information from the currently running configuration (Optional)

Defaults

If no form parameters are specified, the display shows information from the currently running configuration.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show accesslist` or `show accesslist` from `runningconfig` command to display a list of all access lists from the current running configuration.

Use the **all** keyword to display the contents of all access lists.

Use the **from bootconfig** keywords to display the specified access list information as it exists in the current saved configuration, used when the storage router restarts. This may differ from the running configuration.

Examples

To display a list of access lists, issue this command:

```
show accesslist
```

To display the contents of all access lists from the current running configuration, issue this command:

```
show accesslist all
```

To display the contents of all access lists as they exist in the current saved configuration, issue this command:

```
show accesslist all from bootconfig
```

To display the contents of the access list named *webserver2* from the current running configuration, issue this command:

```
show accesslist webserver2
```

To display the contents of the access list named *webserver2* as it exists in the saved configuration file *backup_1218*, issue this command:

```
show accesslist webserver2 from backup_1218
```

show debug scsirouter

To display a variety of SCSI router debug information or perform specific troubleshooting activities, use the `show debug scsirouter` command.

Syntax

```
show debug scsirouter {name | all} scsitrace
show debug scsirouter {name | all} tfestatus
show debug scsirouter name tfestatus verbose
show debug scsirouter name target name [lun nn] scsitrace
show debug scsirouter {name | all}
{scsitrace | tfemapping | tfestatus}
show debug scsirouter name tfestatus verbose
show debug scsirouter name target name [lun nn [scsitrace]]
show debug scsirouter name iscsitrace [hex [ascii]]
[first nn | last nn]
show debug scsirouter name iscsitrace short [first nn | last nn]
show debug scsirouter name iscsitrace stats
```

Table 194: Syntax Description

<code>scsirouter name</code>	The name of the SCSI routing instance.
<code>all</code>	Display information for all SCSI routing instances.
<code>scsitrace</code>	Display raw SCSI trace information for the specified SCSI routing instance or target and LUN combination.
<code>tfemapping</code>	Display target to physical device mapping information.
<code>tfestatus</code>	Display the status of the trace configuration for the specified SCSI routing instance.
<code>verbose</code>	Display detailed information (including management, target management and LUN management tables for all initiators) about the status of the trace configuration for the specified SCSI routing instance.
<code>target name</code>	The name of the target associated with the specified SCSI routing instance.
<code>lun nn</code>	The target LUN number.
<code>iscsitrace</code>	Display iSCSI trace facility output.
<code>hex</code>	Display iSCSI trace data in hex.

Table 194: Syntax Description (Continued)

<code>ascii</code>	Display iSCSI trace data in hex and ASCII.
<code>first nn</code>	Display the specified number of Protocol Data Units (PDUs) from the start of the trace.
<code>last nn</code>	Display the specified number of PDUs from the end of the trace.
<code>short</code>	Display the trace data in a short format.
<code>stats</code>	Display iSCSI trace statistics.

Defaults

None.

Command Modes

Administrator Monitor

Usage Guidelines

To enable trace facilities for debugging SCSI routing instances, use the `debug scsirouter` command.

Some `show debug scsirouter` commands may perform actions that drop existing connections or otherwise impact normal storage router performance. The `show debug scsirouter` command is designed for debug purposes, and should only be used under the guidance of a HP Technical Support professional.

Examples

The following example displays TFE status data for the SCSI routing instance named *foo*:

```
show debug scsirouter foo tfestatus
```


The following is example output displaying the target to physical device mapping information for the SCSI routing instance named *zeus*:

```
show debug scsirouter zeus tfemapping
```

```
TARGET:0x0:chimaera_apps addressMapType=MAP_TYPE_LUNMAP (lun mapping)
```

```
  LUN:0x11: iSCSI2ByteLun=0x11, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWNN
```

```
    Lun ID Length=8 lun ID=0x200000204819137b 00
```

```
    I: NO iSCSI Initiators Logged into target:0x0:chimaera_apps
```

```
  LUN:0x18: iSCSI2ByteLun=0x18, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWPN_LUN
```

```
    WWPN=0x22000020 0x37281505, secWWPN=0x22000020 0x37191505
```

```
    I: NO iSCSI Initiators Logged into target:0x0:chimaera_apps
```

```
  LUN:0x1f: iSCSI2ByteLun=0x1f, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWPN_LUN
```

```
    WWPN=0x22000020 0x37447b0e, secWWPN=0x22000020 0x37559b0e
```

```
    I: NO iSCSI Initiators Logged into target:0x0:chimaera_apps
```

```
TARGET:0x1:chimaera_eng addressMapType=MAP_TYPE_LUNMAP (lun mapping)
```

```
  LUN:0x11: iSCSI2ByteLun=0x11, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWNN
```

```
    Lun ID Length=8 lun ID=0x20000004cf4304cd 00
```

```
    I: NO iSCSI Initiators Logged into target:0x1:chimaera_eng
```

```
TARGET:0x2:pegasus_web addressMapType=MAP_TYPE_LUNMAP (lun mapping)
```

```
  LUN:0x3: iSCSI2ByteLun=0x3, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_SERIAL_NUMBER
```

```
    lunSerialNumber=LS09311I0000I947ZDB5
```

```
    I: NO iSCSI Initiators Logged into target:0x2:pegasus_web
```

```
TARGET:0x3:pegasus_email addressMapType=MAP_TYPE_WWPN (target mapping)
```

```
  WorldWidePortName = 0x22000020 0x371912da, Secondary
WorldWidePortName 0x22000020 0x371912da
```

```
  LUN:0x0: iSCSI2ByteLun=0x0, iScsiLun=0x0000000000000000,
addressMapType=MAP_TYPE_WWPN_LUN
```

```
    WWPN=0x22000020 0x371912da, secWWPN=0x22000020 0x372642da
```

```
    I: NO iSCSI Initiators Logged into target:0x3:pegasus_email
```

The following example of an iSCSI trace display for connections to and from the SCSI routing instance named *sr1* shows a simple login exchange. The display is formatted in hex and ASCII.

```
show debug scsirouter sr1 iscsitrace hex ascii
 1: 10.1.50.12:1912 -> 10.1.50.100:3260, len 252, time 0.000
0000: 43 87 00 00 00 00 00 00 cb 33 39 63 35 00 00 00
00 C.....39c5....
0010: 00 01 00 00 00 01 00 00 00 00 00 01 00 00 00
00 .....
0020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 .....
0030: 54 61 72 67 65 74 4e 61 6d 65 3d 69 71 6e 2e
31 TargetName=iqn.1
0040: 39 38 37 2d 30 35 2e 63 6f 6d 2e 63 69 73 63
6f 987-05.com.cisco
0050: 3a 30 30 2e 36 62 39 35 65 39 33 64 62 62 30
39 :00.6b95e93dbb09
0060: 2e 74 31 00 4d 61 78 52 65 63 76 44 61 74 61
53 .t1.MaxRecvDataS
0070: 65 67 6d 65 6e 74 4c 65 6e 67 74 68 3d 30 78
31 egmentLength=0x1
0080: 30 30 30 30 00 49 6e 69 74 69 61 6c 52 32 54
3d 0000.InitialR2T=
0090: 4e 6f 00 49 6e 69 74 69 61 74 6f 72 4e 61 6d
65 No.InitiatorName
00a0: 3d 69 73 63 73 69 2e 63 69 73 63 6f 2e 64 61
76 =iscsi.cisco.dav
00b0: 61 76 68 6f 2d 6c 6e 78 2e 63 69 73 63 6f 2e
63 avho-lnx.cisco.c
00c0: 6f 6d 00 49 6e 69 74 69 61 74 6f 72 41 6c 69
61 om.InitiatorAlia
00d0: 73 3d 64 61 76 61 76 68 6f 2d 6c 6e 78 2e 63
69 s=davavho-lnx.ci
00e0: 73 63 6f 2e 63 6f 6d 00 53 65 73 73 69 6f 6e
54 sco.com.SessionT
00f0: 79 70 65 3d 6e 6f 72 6d 61 6c 00
00 ype=normal..

 2: 10.1.50.100:3260 -> 10.1.50.12:1912, len 132, time 0.000
0000: 23 87 00 00 00 00 00 00 54 33 39 63 35 00 00 01
#.....T39c5....
0010: 00 01 00 00 00 00 00 00 00 00 00 00 00 00 01
.....
0020: 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00
.....
```

```
0030: 54 61 72 67 65 74 50 6f 72 74 61 6c 47 72 6f 75
TargetPortalGrou
0040: 70 54 61 67 3d 31 00 4d 61 78 52 65 63 76 44 61
pTag=1.MaxRecvDa
0050: 74 61 53 65 67 6d 65 6e 74 4c 65 6e 67 74 68 3d
taSegmentLength=
0060: 35 32 34 32 38 38 00 49 6e 69 74 69 61 6c 52 32
524288.InitialR2
0070: 54 3d 4e 6f 00 54 61 72 67 65 74 41 6c 69 61 73
T=No.TargetAlias
0080: 3d 74 31 00                                =t1.
```

The following is example output displaying short iSCSI trace information for the SCSI routing instance named *sr1*:

```
show debug scsirouter sr1 iscsitrace short
1(0.000): 10.1.50.12:1233 10.1.50.101:3260 10000 LOGIN/I 260 T
CSG=ON NSG=FFP
2(0.000): 10.1.50.101:3260 10.1.50.12:1233 10000 LOGIN-RSP 144 T
CSG=ON NSG=FFP ver=0 OK
3(0.000): 10.1.50.12:1233 10.1.50.101:3260 1020000 SCSI-CMD 0
dlen=0
4(0.900): 10.1.50.101:3260 10.1.50.12:1233 1020000 SCSI-RSP 28 F
stat=2
5(0.900): 10.1.50.12:1233 10.1.50.101:3260 2030000 SCSI-CMD 0
dlen=0
6(0.900): 10.1.50.101:3260 10.1.50.12:1233 2030000 SCSI-RSP 0 F
stat=0
7(14.366): 10.1.50.12:1233 10.1.50.101:3260 3040000 TEXT 16
8(14.366): 10.1.50.101:3260 10.1.50.12:1233 3040000 TEXT-RSP 0
9(24.550): 10.1.50.12:1233 10.1.50.101:3260 4050000 NOP-OUT 1500 F
10(24.550): 10.1.50.101:3260 10.1.50.12:1233 4050000 NOP-IN 1500 F
11(28.050): 10.1.50.12:1233 10.1.50.101:3260 5060000 SCSI-CMD 0 F W
dlen=512
12(33.900): 10.1.50.101:3260 10.1.50.110:1026 ffffffff NOP-IN 0 F
ttt=0
13(33.900): 10.1.50.101:3260 10.1.50.110:1029 ffffffff NOP-IN 0 F
ttt=0
14(33.900): 10.1.50.110:1026 10.1.50.101:3260 ffffffff NOP-OUT/I 0
ttt=0
15(33.900): 10.1.50.110:1029 10.1.50.101:3260 ffffffff NOP-OUT/I 0
ttt=0
16(34.200): 10.1.50.12:1233 10.1.50.101:3260 6070000 SCSI-CMD 0 F W
dlen=512
17(34.200): 10.1.50.101:3260 10.1.50.12:1233 6070000 R2T 0 F
offset=0 desDlen=512
18(34.200): 10.1.50.12:1233 10.1.50.101:3260 6070000 SCSI-DATA-OUT
512 F
19(34.216): 10.1.50.101:3260 10.1.50.12:1233 6070000 SCSI-RSP 0 F
stat=0
20(35.700): 10.1.50.12:1233 10.1.50.101:3260 7080000 SCSI-CMD 0 F R
dlen=512
21(35.700): 10.1.50.101:3260 10.1.50.12:1233 7080000 SCSI-DATA-IN
512 F
22(35.700): 10.1.50.101:3260 10.1.50.12:1233 7080000 SCSI-RSP 0 F
stat=0
```

show debug fcip

To display a variety of debug information or perform specific troubleshooting activities for FCIP instances, use the **show debug fcip** command.

Syntax

```
show debug fcip name {mailboxtrace | packettrace}
```

Table 195: Syntax Description

name	The name of the FCIP instance. Valid names are <i>fcip1</i> and <i>fcip2</i> .
mailboxtrace	Display mailbox trace data.
packettrace	Display packet trace data. The packet trace mask can be set for the current session using the debug fcip command. To retain the packet trace mask setting over a storage router restart, use the fcip destination config command.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.2.1	This command was introduced for the HP SR2122-2.

Usage Guidelines

Use this command to display debugging information for FCIP instances. The **show debug** command is designed for debug purposes and should be used under the guidance of a Cisco Technical Support professional.

Examples

The following is example mailbox trace data for the FCIP instance named *fcip1*:

```
[HP SR2122-2]# show debug fcip fcip1 mailboxtrace
qlpt 0xca99f98, unit 1
linkState Down, linkIsUp FALSE
Peer 0.0.0.0, isConnected TRUE
InitBlock values:
    Max IOCB Allocation 256, Max Frame Length 2112
    Execution Throttle 16, Retry Count 8
    Retry Delay 1, Inquiry Data 0
    Risc Option 0x8000, Additional Firmware Option 0x10
    Special Firmware Option 0x6000
FW_Rev 3.100.101, FW_State 0x4
pktTraceMask 0x0
mboxTracing Yes, cmdCount 0
requestQ: queue_base = 0xca92000
reqinptr = 28, reqoutptr = 0
reqInAbsAddress = 0xca92700, reqOutAbsAddress = 0xca92000
responseQ: queue_base = 0xca8c000
respinptr = 28, respoutptr = 28
respInAbsAddress = 0xca8c700, respOutAbsAddress = 0xca8c700

046: 40 8 - 0
      0009 9d40 0ca8 b000 0040 0000 0000 0000 0000
047: 41 1 - 0
      4000 1111 2222 3333 4444 5555 6666 7777 ffff
048: 40 8 - 0
      0009 9d80 0ca8 b000 0040 0000 0000 0000 0000
049: 41 1 - 0
      4000 1111 2222 3333 4444 5555 6666 7777 ffff
050: 40 8 - 0
      0009 9dc0 0ca8 b000 0040 0000 0000 0000 0000
051: 41 1 - 0
      4000 1111 2222 3333 4444 5555 6666 7777 ffff
052: 40 2 - 0
      0007 0800 0ca8 b000 0040 0000 0000 0000 0000
...
```

Related Commands

Command	Description
<code>debug fcip</code>	Enable debugging for the named FCIP instance.
<code>fcip</code>	Create an FCIP instance.
<code>fcip destination config</code>	Configure operational parameters for the named FCIP instance.
<code>show fcip</code>	Display configuration and operational information for the named FCIP instance.

show scsirouter

To display configuration information and operational statistics related to all SCSI routing instances or the named SCSI routing instance, use the `show`

Syntax

`scsirouter` **command**.

```

show scsirouter
show scsirouter name all
show scsirouter {name | all} [from {bootconfig | runningconfig |
filename}]
show scsirouter {name | all} brief
show scsirouter {name | all} connection [stats | tcp]
show scsirouter {name | all} [serverif] [from {bootconfig |
runningconfig | filename}]
show scsirouter {name | all} failover
show scsirouter {name | all} host [stats]
show scsirouter {name | all} stats
show scsirouter {name | all} target {name | all} [from
{bootconfig | runningconfig | filename} | stats]
```

Table 196: Syntax Description

name (?)	The name of the SCSI routing instance or the name of the target
name all	Displays all configuration information about the specified SCSI routing instance
all	The keyword used to display the requested information about all instances of SCSI routing services or all targets
from bootconfig	Displays the requested SCSI routing services configuration information from the persistent saved configuration (Optional)
from <i>running config</i>	Displays the requested SCSI routing services configuration information from the currently running configuration (Optional)
from <i>filename</i>	The name of the saved configuration file containing the specified SCSI routing instance information. This file must exist in the savedconfig directory. (Optional)
brief	Displays brief configuration information (Optional)
connection	The keyword used to display connection information for the named SCSI routing instance or client, or all instances or clients (Optional)
failover	Displays the HA failover list for the named SCSI routing instance, or all SCSI routing instances (Optional)
hosts	Displays server status and other operational data for hosts currently connected to the named SCSI routing instance (Optional)
serverif	Restricts display to configuration information for interfaces between the named SCSI routing instance and servers (Optional)
servers	The keyword used to display information about the storage router providing the iSCSI client access to storage devices (Optional)
stats	Displays accumulated operational information about the SCSI routing instance or client (including connections, hosts or targets). This display shows statistics accumulated since the named SCSI routing instance became active or statistics were last cleared, whichever is more recent. (Optional)
target	Restricts the display to configuration information related to targets associated with the SCSI routing instance or client, or all instances or clients (Optional)
tcp	The keyword used to display current and maximum TCP window size for each connected host (Optional)

Defaults

The `show scsirouter` command with no parameters displays the name of each SCSI routing instance running on this storage router. When no form parameters are specified, the information displayed is from the currently running configuration.

Command Modes

Administrator or Monitor.

Usage Guidelines

In a cluster environment, a storage router that is currently running a SCSI routing instance is known as the current primary for that instance. Issue the appropriate `show` commands from this storage router to display complete configuration information and operational statistics for the active SCSI routing instance. If you issue `show` commands from the storage router that is not running the instance, operational statistics are not available and configuration information is truncated.

Use the optional keywords **target** and **serverif** to restrict the display to SCSI routing services configuration information related to those objects. For example:

- The command `show scsirouter name target` displays current configuration information for all targets associated with the named instance, including access lists.
- The command `show scsirouter all serverif` displays current configuration information for interfaces between all SCSI routing services and the servers/hosts.

Use the **connection** or **host** keywords to display specific operational data for the named instance or all instances of SCSI routing services.

- The command `show scsirouter name host stats` displays server status and operational statistics for currently connected hosts for the named SCSI routing services, if the server status is active.
- The command `show scsirouter name stats` displays accumulated operational information about all hosts that have been connected since the named instance became active. Operational statistics include login information, host-to-router and router-to-host statistics, followed by a roll-up of selected statistics for quick reference.
- The `show scsirouter all stats` command is useful for determining quick operational status of all SCSI routing services running in the storage router.

- Use the `show scsirouter all` command to display configuration information for all SCSI routing services, including descriptions, targets and associated access lists.

Examples

The following is example output from the `show scsirouter` command:

```
show scsirouter
  foo1
  foo2
```

The following is example output from the `show scsirouter host stats` command:

```
show scsirouter server2 host stats
  0 hosts listed
```

[Table 197](#) describes the significant fields shown in the display.

Table 197: show scsirouter host stats Field Description

Field	Description
SrvState	The current server state (active or inactive). If the server is active, connected host information is also displayed.
Uptime	The elapsed amount of time the system has been active, in seconds
StartTime	The date the server was last started
ConnsAccepted	The total number of connections accepted since the last time the system was started
ConnsOpen	The total number of connections that are currently open
SessionsActive	The total number of sessions that are currently active
IpAddr	The IP address of the connected host
TcpPort	The TCP port number for this connection
SessionId	A pair of numbers that uniquely identify this session
HConnState	The state of the host connection (NotLoggedIn or FullPhase)
Rtt	On or off
HConnElapsed	The total Amount of time this host has been connected, in seconds
HConnDate	The date this connection was established

Table 197: show scsirouter host stats Field Description (Continued)

Field	Description
HrxDataBytes	The total amount of data received from host on this connection, in bytes
HtxDataBytes	The total amount of data transmitted to the hosts on this connection, in bytes
HScsiCmdsRej	The total number of SCSI commands rejected on this connection

The following is an example output from the `show scsirouter stats` command:

```
show scsirouter all stats
router      status      started   version   logins    active
aaa         INACTIVE
RAID        INACTIVE
blue        INACTIVE
black       INACTIVE
AAA         INACTIVE
purple I    INACTIVE
yellow      INACTIVE
ht-dataver  INACTIVE
oracle-sun  INACTIVE
oracle-sunfs INACTIVE
red         INACTIVE
11 scsirouters listed
```

Table 198: show scsirouter stats Field Description

Field	Description
IpAddr	The IP address of the connected host
InitiatorName	The name of the initiator. This field is usually blank.
LoginsActive	The total number of active logins for this instance
LastLoginTime	The date and time the last login occurred
LoginsTerminated	The total number of logins terminated
LastLoginTerminationTime	The date and time the last login termination occurred
RxTotMsgs	The total number of messages received from this host
RxNopMsgs	The total number of no-op messages received
PingCmdMsgs	The total number of "ping" command messages exchanged

Table 198: show scsirouter stats Field Description (Continued)

Field	Description
ScsiCmdMsgs	The total number of SCSI commands received
ScsiCmdsRej	The total number of SCSI commands rejected
RxScsiDataMsgs	The total number of SCSI data messages received
ScsiDataMsgsRejected	The total number of SCSI data messages rejected
RxScsiDataBytes	The total amount of SCSI data received from this host, in bytes
ScsiDataBytesDiscarded	The total amount of SCSI data discarded from this host, in bytes
TaskMgtMsgs	The total number of task management messages exchanged
TaskMgtMsgsRej	The total number of task management messages rejected
LoginCmdMsgs	The total number of login command messages exchanged
LoginCmdMsgsRej	The total number of login command messages rejected
TextCmdMsgs	The total number of text command messages received
TextCmdMsgsRej	The total number of text command messages rejected
InvalidMsgs	The total number of "invalid Op Code" messages received
TxTotMsgs	The total number of messages transmitted to this host
TxNopMsgs	The total number of no-op messages transmitted to this host
PingRspMsgs	The total number of responses issued to "ping" commands
LoginRspMsgs	The total number of responses to login messages
TextRspMsgs	The total number of responses to text command messages
InvOpcodeMsgs	The total number of responses to "invalid Op Code" messages
RttMsgs	The total number of RTT messages sent to this host
ScsiRspMsgs	The total number of responses to all SCSI messages
TxScsiDataMsgs	The total number of SCSI data messages transmitted to this host

Table 198: show scsirouter stats Field Description (Continued)

Field	Description
TxScsiDataBytes	The total amount of data transmitted to this host, in bytes
ScsiTaskMgtRspMsgs	The total number of responses to task management messages
AsyncEvtMsgs	The total number of unsolicited messages transmitted to this host
TotalRxMsgs	The total number of messages received for this instance
TotalTxMsgs	The total number of messages transmitted for this instance
TotalRxDataBtes	The total amount of data received for this instance, in bytes
TotalTxDataBytes	The total amount of data transmitted for this instance, in bytes
TotalAsyncMsgs	The total number of unsolicited messages transmitted for this instance
TotalScsiCmdMsgs	The total number of SCSI command messages received for this instance
TotalScsiCmdMsgsRej	The total number of SCSI command messages rejected for this instance
TotalInvalidMsgs	The total number of "invalid Op Code" messages received for this instance

show slp

To display the status of the Service Location Protocol (SLP) service and the interface address where the SLP service is listening for incoming SLP service requests, use the **show slp** command.

```
show slp
```

Syntax Description

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to display the operational status of the SLP service. The SLP listens on all configured IP interfaces.

Examples

The following is example output from the **show slp** command:

```
[HP SR2122-4A]# show slp
SLP is RUNNING
Listening interfaces:
      127.0.0.1          TCP LISTEN
      10.1.40.116       TCP LISTEN      UDP MULTICAST      UDP
UNICAST
      10.1.20.116       TCP LISTEN      UDP MULTICAST      UDP
UNICAST
```

Related Commands

Command	Description
<code>scsirouter slp enable</code>	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
<code>slp findattrsslp findattrs</code>	Discover the attributes of a specific SLP registered service.
<code>slp findsrvs</code>	Locate a SLP registered service of a specific type on the local subnet.
<code>slp findsrvtypes</code>	Discover all SLP registered service types on the local subnet.

show static

To display the currently configured IP host to Fibre Channel (FC) address mappings saved in the storage router, use the **show static** command. This command is only available when the storage router is deployed for static transparent SCSI routing.

Syntax

```
show static iscsibindings
```

Table 199: Syntax Description

<code>iscsibindings</code>	Display the IP host to FC mappings that are currently configured in the storage router.
----------------------------	---

Defaults

None.

Command Modes

Administrator and Monitor.

Command History

Release	Modification
3.3.1	This command was introduced.

User Guidelines

When the storage router is deployed for static transparent SCSI routing, the IP host to FC address mappings are saved and retained in the storage router when it is restarted. Use the **show static iscsibindings** command to display the mappings that are currently configured in the storage router.

Examples

The following example displays the currently configured mappings:

```
[HP SR2122-2]# show static iscsibindings
Interface WWPN                      Host IP Address  Host Name
-----
-----
fci1      280100065338d6c0 10.1.20.2       iscsi.cisco.testlab
fci1      280200065338d6c0 10.1.4.213      iqn.1987-05.com.cisco.
02.0AB08...B6E5CCE.WIN1
fci2      290100065338d6c0 10.1.30.100     iqn.1987-05.com.cisco.
02.9FD389...36D3D3.NT10

Interface Autolearn
-----
fci1      enabled
fci2      enabled
```


Related Commands

Command	Description
<code>clear static</code>	Clear the mapping of the IP host to Fibre Channel (FC) address for the specified WWPN.
<code>static iscsibinding interface autolearn</code>	Enable and disable auto-learning of static WWPN bindings.
<code>static iscsibinding interface index</code>	Manually populate the iSCSI static binding table for the specified interface.

slp findattrs

To discover the attributes of a specific Service Location Protocol (SLP) registered service, use the **slp findattrs** command.

Syntax

```
slp findattrs service [attribute]
```

Table 200: Syntax Description

<code>service</code>	The SLP service. Use the slp findsrvs command to locate the specific service.
<code>attribute</code>	Display the value of the specified service attribute.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

User Guidelines

Use this command to verify that the attributes of advertised targets associated with a SCSI routing instance are correct.

Use the **slp findsrvs** command to display the service information used as arguments in the command.

Examples

The following example discovers the attributes of all *iscsi:target* services:

```
[HP SR2122-2]# slp findattr iscsi:target
```

```
(iscsi-name=iqn.1987-05.com.cisco:00.dd6b75bc42ef.chimaera_apps), (
alias=chimaera_apps),
(portal-group=1), (auth-addr=any), (auth-name=an)
(iscsi-name=iqn.1987-05.com.cisco:00.d621b8e50a31.chimaera_web), (a
lias=chimaera_web),
(portal-group=1), (auth-a)
```

The following example discovers the value of the *alias* attribute for all *iscsi:target* services:

```
[HP SR2122-2]# slp findattr iscsi:target alias
```

```
(alias=chimaera_apps)
(alias=chimaera_web)
```

Related Commands

Command	Description
<code>scsirouter slp enable</code>	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
<code>show slp</code>	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
<code>slp findsrvs</code>	Locate a SLP registered service of a specific type on the local subnet.
<code>slp findsrvtypes</code>	Discover all SLP registered service types on the local subnet.

slp findsrvs

To locate a Service Location Protocol (SLP) registered service of a specific type on the local subnet where the storage router is located, use the **slp findsrvs** command.

Syntax

```
slp findsrvs service [(attribute=value)]
```

Table 201: Syntax Description

<code>service</code>	The SLP service type. For example, the SLP service type for iSCSI targets is <i>iscsi:target</i> .
<code>attribute=value</code>	Display the specified service attribute value pair. The attribute value pair must be displayed in parenthesis.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

Usage Guidelines

Use this command to verify that a SCSI routing instance that is enabled for SLP is registering its accessible targets with the SLP service. The command displays the URLs for the specified SLP registered service types if they are available on the local subnet.

To display a list of all SLP registered service types found on the local subnet, use the **slp findsrvtypes** command. To display attributes for a specific SLP registered service, use the **slp findattrs** command.

Examples

The following is example output from the **slp findsrvs** command. In this example, two targets are found at address 10.1.10.10. The URL includes the iSCSI Name for each target. The targets belong to a SCSI routing instance with a Gigabit Ethernet interface IP address of 10.1.10.10. The SCSI routing instance may be located on the local storage router or on another storage router in the network.

```
[HP SR2122-2]# slp findsrvs iscsi:target
```

```
service:iscsi:target://10.1.10.10:3260/iqn.1987-05.com.cisco:00.d8  
75b8262ff6.disk1,64432  
service:iscsi:target://10.1.10.10:3260/iqn.1987-05.com.cisco:00.bd  
0e6aa3eb51.disk2,64432
```

The following example discovers all SCSI routing instance targets with an alias of *disk1*:

```
[HP SR2122-2]# slp findsrvs iscsi:target (alias=disk1)
```

```
service:iscsi:target://10.1.10.10:3260/iqn.1987-05.com.cisco:00.d8  
75b8262ff6.disk1,64432
```

Related Commands

Command	Description
<code>scsirouter slp enable</code>	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
<code>show slp</code>	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
<code>slp findattrs</code>	Discover the attributes of a specific SLP registered service.
<code>slp findsrvtypes</code>	Discover all SLP registered service types on the local subnet.

slp findsrvtypes

To discover all Service Location Protocol (SLP) registered services on the local subnet where the storage router is located, use the **slp findsrvtypes** command.

Syntax

```
slp findsrvtypes
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Command History

Release	Modification
3.2.1	This command was introduced.

User Guidelines

Use this command to invoke an SLP user agent tool which looks for SLP registered services on the local subnet. If any SLP services are found, a list of the service types and URLs displays. If SCSI routing instances have SLP enabled and have targets advertised with SLP, the display lists an available SLP service of type *iscsi:target*.

Examples

The following is example output from the **slp findsrvtypes** command:

```
[HP SR2122-2]# slp findsrvtypes
service:iscsi:target
```

Related Commands

Command	Description
<code>scsirouter slp enable</code>	Enable the advertisement of the targets of the named SCSI routing instance with the SLP service.
<code>show slp</code>	Display the status of the SLP service and the interface address where the SLP service is listening for incoming SLP service requests.
<code>slp findattr</code>	Discover the attributes of a specific SLP registered service.
<code>slp findsrvs</code>	Locate a SLP registered service of a specific type on the local subnet.

static iscsibinding interface autolearn

To enable and disable auto-learning of static WWPN bindings, use the **static iscsibinding interface autolearn** command. This command is only available when the storage router is deployed for static transparent SCSI routing.

Syntax

```
static iscsibinding interface fci? autolearn {enable | disable}
```

Table 202: Syntax Description

fci?	The name of the interface for which auto-learning is enabled or disabled. Valid values are fci1 or fci2. When you type the static iscsibinding interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
enable	Enable auto-learning of iSCSI targets.
disable	Disable auto-learning of iSCSI targets.

Defaults

Auto-learning of iSCSI targets is enabled.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced.

Usage Guidelines

When the storage router is deployed for static transparent SCSI routing, the IP host to FC address mappings are saved and retained in the storage router when it is restarted. By default, IP hosts attempting to access storage automatically learn the available iSCSI WWPN bindings. Use the **static iscsibinding interface autolearn** command to disable the auto-learn feature. When the auto-learn feature is disabled, the IP host must have a specific IP host to FC address mapping configured in the iSCSI static binding table.

When you enable or disable the auto-learn feature for one internal FC interface (for example, fci1), the same setting is applied to the other internal FC interface (for example, fci2).

To display the mappings that are currently configured in the storage router, use the **show static iscsibindings** command.

Examples

The following example disables the auto-learn feature. All IP hosts must have specific host to FC address mappings configured in the iSCSI static binding table to access storage.

```
[HP SR2122-2]# static iscsibinding interface fci2 autolearn disable
```

Related Commands

Command	Description
<code>clear static</code>	Clear the mapping of the IP host to Fibre Channel (FC) address for the specified WWPN.
<code>show static</code>	Display the currently configured IP host to FC address mappings saved in the storage router.
<code>static iscsibinding interface index</code>	Manually populate the iSCSI static binding table for the specified interface.

static iscsibinding interface index

To manually populate the iSCSI static binding table for the specified interface, use the **static iscsibinding interface index** command. This command is only available when the storage router is deployed for static transparent SCSI routing.

Syntax

```
static iscsibinding interface fci? index nn ip-address A.B.C.D  
iscsi-name name
```


Table 203: Syntax Description

fc1?	The name of the interface. Valid values are fc1 or fc2. When you type the static iscsibinding interface fc? command, the CLI lists the interfaces available. You cannot specify a nonexistent interface.
index nn	The multi-initiator virtual port number. Enter a value between 1 and 31.
ip-address A.B.C.D	The IP address of the host that will use the static iSCSI binding.
iscsi-name name	The iSCSI Name of the initiator.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
3.4.1	This command was introduced.

When the storage router is deployed for static transparent SCSI routing, the IP host to FC address mappings are saved and retained in the storage router when it is restarted. Use the **static iscsibinding interface index** command to manually add a mapping to the iSCSI static binding table.

To display the mappings that are currently configured in the storage router, use the **show static iscsibindings** command.

Examples

The following example adds a static mapping for the IP host at *10.1.40.23*, using the internal FC interface, *fc12*:

```
[HP SR2122A]# static iscsibinding interface fc12 index 1 ip-address
10.1.40.23 iscsi-name vt1
```

Related Commands

Command	Description
<code>clear static</code>	Clear the mapping of the IP host to Fibre Channel (FC) address for the specified WWPN.
<code>show static</code>	Display the currently configured IP host to FC address mappings saved in the storage router.
<code>static iscsibinding interface autolearn</code>	Enable and disable auto-learning of static WWPN bindings.

SNMP Commands

14

This section describes all the CLI commands related to SNMP. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

show snmp

To display SNMP management configuration information for the storage router, use the `show snmp` command.

Syntax

```
show snmp
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show snmp` command to review the SNMP configuration setting before changing those setting with the `snmp-server` command.

The command displays IP addresses or host names of the destination hosts used for notifications (traps), the name of the SNMP community having read access to the SR 2122 network (get-community), and the name of the community having write access to the SR 2122 network (set-community), the version of traps to be sent, and configuration information for Send Authentication and Link Up/Down traps.

Examples

The following is an example output from the `show snmp` command:

```
show snmp
First Trap Host: <none found or defined>
Second Trap Host: <none found or defined>
Get Community String: public
Set Community String: private
Send Authentication Traps: disabled
Link Up/Down Enable for mgmt: enabled
Link Up/Down Enable for ha: enabled
Link Up/Down Enable for fc1: enabled
Link Up/Down Enable for ge2: enabled
```

snmp-server

To configure SNMP management on the storage router, use the `snmp-server` command. To disable SNMP management, or specific host or traps, use the `no` forms of this command.

Syntax

```
snmp-server community community-name {ro | rw}
snmp-server host A.B.C.D [version nn traps]
snmp-server {linkupdown {all | ifname} | sendauthtraps}
no snmp-server host {all | A.B.C.D} traps
no snmp-server {linkupdown | all | ifname | sendauthtraps}
```

Table 204: Syntax Description

community-name	The name of the community having the specified access (read or write) to the SR 2122 network. Enclose the string in quotation marks.
ro	The keyword signifying read-only access. The storage router will respond to this community's GET commands. The default SNMP getcommunity is public.
rw	The keyword signifying read-write access. The storage router will respond to this community's SET commands. The default SNMP setcommunity is private.

Table 204: Syntax Description (Continued)

A.B.C.D	The IP address of the primary (or first) destination host used for notifications (traps). A.B.C.D is the dotted quad notation of the IP address. If the command is issued twice, the second IP address becomes the secondary destination host used for notifications. Version 1 traps will be sent by default.
version nn(?)	Specifies the SNMP version for the traps (Optional)
linkupdown all	The keywords used to enable or disable SNMP link Up/Down traps for all interfaces
linkupdown ifname	The keyword used to enable or disable SNMP link Up/Down traps for the specified interface
sendauthtraps	The keyword used to enable or disable sending of authorization failure traps sent when a SNMP request is received with an incorrect community name
host all	Removes all destination hosts used for SNMP notifications (traps)

Defaults

The default read-only community name is “**public**.” This is also known as the *getcommunity*. The default read-write community name is “**private**.” This is also known as *setcommunity*. SNMP notifications are disabled by default.

Command Modes

Administrator.

Usage Guidelines

A variety of network management methods may be used with the storage router, including SNMP. All management methods are enabled by default.

The first issuance of the `snmp-server host` command sets the primary destination host used for traps; the second issuance of the command sets the secondary destination host. Version 1 traps are sent by default. To send other trap versions, use the `snmp-server host` command with the **version** keyword.

Link Up/Down traps can be sent for any valid storage router interface.

Table 205: snmp-serverif-name

Keyword	Description
mgmt	The management interface
ha	The HA interface
ge?	The Gigabit Ethernet interface; for example, ge2
fc?	The Fibre Channel interface; for example, fc1

Examples

The following command identifies the IP address *10.3.4.200* as the primary destination for SNMP Version 1 traps:

```
snmp-server host 10.3.4.200 traps
```

The following command enables the storage router to send authorization failure traps to the SNMP destination host:

```
snmp-server sendauthtraps
```

The following command enables the storage router to send SNMP link Up/Down traps for all interfaces to the SNMP destination host :

```
snmp-server linkupdown all
```


Software Management Commands

15

This section describes all the CLI commands related to the software management feature in the system. The no form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, history, usage guidelines, examples, and related commands.

copy http

To copy a named configuration file or script file to the `savedconfig` or `script` directory via HTTP, use the `copy http` command. When copying files to the storage router, any file of the same name in the `savedconfig` or `script` directory is overwritten.

Syntax

```
copy http://FileUrl savedconfig:configfilename
copy http://FileUrl script:filename
```

Table 206: Syntax Description

http	The keyword, indicating the HTTP protocol is being used to transfer the named file
saved config	The keyword, indicating the named file resides in the savedconfig directory
script	The keyword, indicating the named file resides in the script directory
FileUrl	The URL (including the file name) of the configuration or script file to be copied to the storage router, such as http://acme/~myhome/all.conf.xml . (In this example, the host name acme can be used if the ip name-server command was previously issued.)
config filename	The name of the saved configuration file
filename	The name of the saved script file

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Configuration files are specially formatted XML files. The `copy http` command verifies that the specified file is of the required format.

Copying a file into the `savedconfig` directory does not affect the running or persistent configuration of the storage router or cluster. However, the `restore` command can be used to copy the contents of a saved configuration file into persistent memory, while the `read` command can be used to execute the commands in a script file.

Examples

The following example imports the saved configuration file *myFoo.xml* from server *yourserver*:

```
copy http://yourserver/dir/myFoo.xml savedconfig: myFoo.xml
```

copy tftp

To copy a named configuration file or script file to the `savedconfig` or `script` directory, or from the storage router to the specified location via TFTP, use the `copy tftp` command. When copying files to the storage router, any file of the same name in the `savedconfig` or `script` directory is overwritten.

Syntax

```
copy tftp:location/directory/filename
savedconfig:configfilename

copy tftp:location/directory/filename script:filename

copy savedconfig:configfilename
tftp:location/directory/filename

copy script:filename tftp:/location/directory/filename
```

Table 207: Syntax Description

tftp	The keyword, indicating the Trivial File Transfer Protocol (TFTP) is being used to transfer the named file
saved config	The keyword, indicating the named file resides in the <code>savedconfig</code> directory
script	The keyword, indicating the named file resides in the <code>script</code> directory

Table 207: Syntax Description (Continued)

location	The server name or IP address
directory	The directory name
filename	The name of the file to be copied
config filename	The name of the saved configuration file

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Saved configuration files are specially formatted XML files. The `copy tftp` command verifies that the specified file is of the required format. Script command files are not validated; so it is assumed they contain only valid ASCII text.

The `restore` command can be used to copy the contents of a saved configuration file into persistent memory, while the `read` command can be used to execute the commands in a script file.



WARNING: The `tftp` command does not require user name and password information so it does not allow a user to create directories or files. This means when you export a file using `tftp` the full path must have read/write permissions and must already exist.

Examples

The following example imports the saved configuration file *myFoo.xml* from server *yourserver*:

```
copy tftp:yourserver/dir/myFoo.xml savedconfig:myFoo.xml
```

The following example import script file *initial_SR2122A* from server *yourserver*:

```
copy tftp:yourserver/dir/initial_SR2122A script:initial_SR2122A
```

The following example exports the saved configuration file *myFoo.xml* to another location where the full path to *yourserver/dir/myFoo.xml* must have read/write permissions and already exist:

```
copy savedconfig:myFoo.xml tftp:yourserver/dir/myFoo.xml
```

The following example exports the a script file *initial_SR2122A* to another location where the full path to *yourserver/dir/initial_SR2122A* must have read/write permissions and already exist:

```
copy script:initial_SR2122A tftp:yourserver/dir/initial_SR2122A
```

delete software version

To delete the specified version of software from the storage router, use the `delete software version` command.

Note: The version of software currently running, and the version that will be booted when the system is next restarted, cannot be deleted.

Syntax

```
delete software version version
delete software version all
```

Table 208: Syntax Description

<code>version</code>	The version of storage router software to be deleted
<code>all</code>	Deletes all non-bootable and non-current software versions

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use this command to remove old versions software from the storage router.

Examples

The following example removes version *2.0.1* from the storage router:

```
delete software version 2.0.1
```

download software

To download the specified object from the named location or the default download location, use the `download software list` command.

Syntax

```
download software {http | proxy} list
download software {http | proxy} url full_url
download software {http | proxy} version version
download software tftp hostname host filename file
download software tftp list
download software tftp version version
```

Table 209: Syntax Description

http	Specifies download using the HTTP protocol
proxy	Specifies download using a proxy server
url	Specifies the URL for the download (Optional)
full_url	The fully-qualified URL from which to download this version of storage router software. For example, http://anywebserver.com/2.1.1.tar .
list	Downloads list of available versions (Optional)
version version	Downloads the specified version of storage router software from the default location (Optional)

Table 209: Syntax Description

<code>tftp</code>	Downloads using the TFTP protocol
<code>hostname name</code>	Specifies the name of the TFTP host
<code>filename file</code>	Specifies the name of the file to be downloaded, such as 2.1.1.tar. This file contains the storage router software.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The list of available software versions is stored in the file named *sw-version.txt*. This text file must contain one line for each version of software that is available in the download location. If you store and download software from a site other than the system default (<http://www.hp.com>), create this file and update it whenever a new version of software is available.

Software is downloaded from either the default locations set for the specified protocol or from the location specified as part of the command. Always verify software after it has downloaded to assure no errors were encountered.

A maximum of two versions of software can be stored on the storage router.

Examples

The following example downloads storage router software version 2.1.1 from the default location via standard Hypertext Transfer Protocol (HTTP):

```
download software http version 2.1.1
```

The following example download file named *sr2122v211.tar* from the Trivial File Transport Protocol (TFTP) host named *my_tftpHost*. The file must exist in the default TFTP directory.

```
download software tftp hostname my_tftpHost filename sr2122v211.tar
```

The following file downloads the list of available software from the default location using the storage router's proxy configuration:

```
download software proxy list
```

show software version

To display a list of SR 2122 software versions available on the storage router, use the `show software version` command.

Syntax

```
show software version [all | boot | current | version]
```

Table 210: Syntax Description

all	Displays information about all versions of software available on the storage router (Optional)
boot	Displays only information about the version of software that will be run when the system is rebooted (Optional)
current	Displays only information about the version of software that is currently running on the storage router (Optional)
version	Displays information about the specified software version (Optional)

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show software version` command to display the size of each version of software and the date and time it was built. The display also shows the version of software currently running and the version that will be booted when the system is reset. It includes the protocol and default location from which new software is available for download and the amount of disk space currently available for new software.

Examples

The following is an example output from the `show software version all` command:

```
show software version all
Version  Boot Hash Sign Crash Size      Date
-----  -
2.0.1.7  OK   OK   N/A  0      6.46 MB Jul 13 14:27 CDT 2001
2.1.1    N/A  OK   N/A  0      6.48 MB Jul 18 11:17 CDT 2001

Http Url: http://www.hp.com
Http Username:
Http Password:

Proxy Address:
Proxy Port:
Proxy Url:
Proxy Username:
Proxy Password:

Tftp Hostname:
Tftp Directory:

Disk Space Available: 12.50 Mbytes
Current Version: 2.0.1.7
Boot Version: 2.0.1.7
```

show version

To display version information for system-level software and applications, use the `show version` command.

Syntax

```
show version
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

Use the `show version` command to display version information about the storage router operating system software, system bootstrap, application software, and CLI.

Examples

The following is an example output from the `show version` command:

```
show version
HP SR 2122-sjann Storage Router

Operating System Software Ver: 2.2.0.26
System Bootstrap Ver: 2.2.0.26
Application Software Ver: sjann-G3-2.2.0.91
CLI Version 2.1
```

Copyright (c) 1986-2001 by HP Systems, Inc

software http url

To configure the default location from which to download updated SR 2122 software to the storage router via HTTP protocol, use the `software http url` command.

Syntax

```
software http url {url | default | none}
```

Table 211: Syntax Description

url	The complete URL identifying the location from which to download SR 2122 software (Ex: http://servername/path)
default	Returns this setting to the default download location. The default location is set to http://www.hp.com
none	Deletes the current download location and leaves the URL blank. Use this keyword to prevent software downloads via HTTP protocol

Defaults

The proxy URL is set to “none.”

Command Modes

Administrator.

Usage Guidelines

Updated SR 2122 software is available from the <http://www.hp.com> website. It can also be downloaded and stored locally, then transferred to the storage router when necessary via the `software http url` command.

To see the location defined as the current default download location, issue the `show version all` command.

Examples

The following command specifies the location of the software used to update the SR 2122:

```
software http url http://10.1.01.3/~jsmith/SR2122/v1
```

software http username

To configure an optional user name and password used to retrieve updated storage router software from the HTTP download location, use the `software http username` command. See `software http url` for details on setting the location from which to download software.

Syntax

```
software http username none  
software http username username [password password]
```

Table 212: Syntax Description

username	The user name required to retrieve SR 2122 software from the download location
none	Indicates user name and password are not required. Sets these values to “none.” This is the default string.
password	The password required to retrieve SR 2122 software from the download location (Optional)

Defaults

User name and password are, by default, set to “**none**.”

Command Modes

Administrator.

Usage Guidelines

Use the `show version all` command to display the current user name configured for retrieval of updated storage router software from the HTTP download location.

Use the **none** keyword to indicate that the web server does not require a user name and password to download software, effectively changing the user name and password values to “none.”

Examples

The following example sets the user name for HTTP download to *FooAdmin* and the password to *foo*:

```
software http username FooAdmin password foo
```

software proxy

To configure the address and port of a proxy server to be used when downloading updated SR 2122 software to the storage router via HTTP protocol, use the `software proxy` command.

Syntax

```
software proxy address address [port nn]  
software proxy port nn
```

Table 213: Syntax Description

address	The IP address or URL of the proxy server. To remove a proxy server address, set the address string to blanks using "".
nn	The port number of the proxy server (Optional)

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The proxy server will be used to access the proxy URL for HTTP download of software for the storage router. To change the port specification without changing the address, use the `software proxy port` command. Use the `software proxy url` command to configure the default download location.

Examples

The following example configures the proxy address as *10.1.10.126* and port as *32*:

```
software proxy address 10.1.10.126 port 32
```

software proxy url

To configure the default location from which to download updated SR 2122 software to the storage router via HTTP protocol using the configured proxy server, use the `software proxy url` command.

Syntax

```
software proxy url {url | default | none}
```

Table 214: Syntax Description

url	The complete URL identifying the location from which to download SR 2122 software via the configured proxy server (Ex: http://servername/path)
default	Returns this setting to the default proxy download location. The default location is http://www.hp.com .
none	Deletes the current proxy download location and leaves the URL blank. Use this keyword to prevent software downloads via the proxy server.

Defaults

The proxy URL is set to “none.”

Command Modes

Administrator.

Usage Guidelines

If you use a proxy server to access locations on the Internet, configure the proxy server address and port number using the `software proxy address` command. The proxy server will be used to access the proxy URL when downloading updated storage router software.

Examples

The following example configures the proxy address as `10.1.10.126` and port as `32` and then sets the proxy download URL to <http://www.foo1.com>:

```
software proxy address 10.1.10.126 port 32
software proxy url http://www.foo1.com
```

software proxy username

To configure an optional user name and password used to retrieve updated storage router software from the proxy download location, use the `software proxy username` command. See `software proxy url` for details on setting the location from which to download software.

Syntax

```
software proxy username none  
software proxy username username [password password]
```

Table 215: Syntax Description

username	The user name required to retrieve storage router software from the proxy download location
none	Indicates user name and password are not required. Sets these values to “none.” This is the default setting.
password	The password required to retrieve SR 2122 software from the proxy download location (Optional)

Defaults

User name and password are, by default, set to “**none**.”

Command Modes

Administrator.

Usage Guidelines

Use the `show version all` command to display the current user name used to retrieve updated SR 2122 software from the proxy download location.

Use the **none** keyword to indicate that the web server does not required a user name and password to download software, effectively changing the user name and password values to “none.”

Examples

The following example sets the user name for proxy download to *FooAdmin* and the password to *foo*:

```
software proxy username FooAdmin password foo
```

software tftp

To configure host and filename information used when downloading updated SR 2122 software to the storage router via the Trivial File Transfer Protocol (TFTP), use the `software tftp` command.

Syntax

```
software tftp directory {none | directory}  
software tftp hostname hostname [directory directory]
```

Table 216: Syntax Description

directory	The name of the TFTP base directory. Default is /ata0/software.
hostname	The name of the remote TFTP host. To remove the TFTP configuration, set the host name to blanks using "".
none	Removes the directory setting, effectively disabling the use of TFTP protocol

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use this command to set the required TFTP parameters, effectively enabling software updates via TFTP protocol.

Use the `show software version all` command to display the current TFTP settings.

Examples

The following examples sets the TFTP hostname to *TFTPHost1* and the directory to */SR2122A*:

```
software tftp hostname TFTPHost1 directory /SR2122A
```

software version

To set the version of software to run the next time the system is restarted, use the `software version` command. This command forces a system reset and changes the running version of the SR 2122 software.

Syntax

```
software version version
```

Table 217: Syntax Description

version	The version of storage router software to be run when the system is reset
---------	---

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

This command performs necessary system modifications to assure that the new software version can be run. It causes a system reset; the new version of software will be run when the reset is complete.

In a cluster environment, this command may temporarily suspend normal HA communications, causing a failover of any SCSI routing instances active on this storage router. Any instances with the **primary** attribute set to the IP address of this storage router will resume running on this storage router after it is rebooted.

Use the `show software version all` command to display the list of available versions, the currently running version and the version, that will run the when the system is reset.

Examples

The following is an example output from the `software version` command:

```
software version jsmith3.0.1.18
Module           Size      Status  MD5 Digest
-----
vxWorks          2712103  OK      765c887a567a5765cc59d41d35801089
vxWorks.sym      205115   OK      b689b0e21d8373d8125251bbe434a670
....
Disk Space (required/available): 2980086/7626752 Bytes
```

Please do ***NOT*** shutdown or reboot the system until the software update process completes. A fatal error could occur if you shutdown or reboot the system before the software update process completes.

```
Attempt 1:
Gathering system files... OK
Verifying checksums...   OK
Updating system files...  OK
Updating flash device...  OK
```

The software update process was successful. You must reboot the system in-order for the new software version to take effect.

verify software

To check the specified software version for problems, issue the `verify software` command.

Syntax

```
verify software version {all | boot | current | version}
```

Table 218: Syntax Description

all	Verifies all software versions available to the storage router
boot	The software version that is set to boot at the next system restart
current	The software version currently running
version	A specific version of software, which must be available to the storage router

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use this command after downloading software to verify that the download completed successfully and that the downloaded software is bootable. The size and the status of each module is verified.

Examples

The following is an example output from the `verify software version` command:

```
verify software version 2.1.1
Module              Size      Status   MD5 Digest
-----
-----
vxWorks              2708334 OK
    d51e166af99804c858c0c6592cd46b34
vxWorks.sym          204654  OK
    6a46c358d30408314b0c26af714eb62c
bootrom_uncmp.hex    1340146 OK
    91f75261800c6886dfc8b65d5081601e
sysInit.out          58740   OK
    87797fca4e7c581c10a70a8fa11ded84
crashDump.out        13459   OK
    adc23a6a13188ce9d8da960a597c8d9a
nuUtils.out          55110   OK
    5535e334d121709c1668cb02165ecd0c
nuEvents.out         18528   OK
    ec4aff0c9bd4f5e68ab4019575d047bb
ha.out               30806   OK
    9b6c47ed60430062c0bef52bba1ba914
confNode.out         10776   OK
    3a0e4289b245f42528e78fb9bd9385b6
authServer.out       14910   OK
    c769bfd317289c202eb26b576250e92d
drv.out              29141   OK
    a5df1cda68d4d308a79ebb35e4fc4333
qlogic.out           317383  OK
    4a18ca9abfc7c66754aecb7804f02936
i82543.out           45505   OK
    c06f58bb0e3a8ffbe4f8810ca5ea3620
vtp.out              16885   OK
    a641ccc2d4a16596cc452cc58d8d8ac7
scsiTargetFE.out     66472   OK
    07d53c5ad8304b6013a2b466eed0a793
scsiTargetBE.out     41959   OK
    bd9223e3a239b927e2f2d6b2d295b243
scsiTcpAuth.out      6522    OK
    3e426b83c32481518ec3de3e1be396d1
scsiTcpServer.out    78028   OK
    5fa8517fd4c586b7032a4fca10e5ab7b
scsiTcpClient.out    55782   OK
```

```
bab9732ee80bdcf018f2f28fdccdc9fd
ttcp.out          22137    OK
5d596240993cbf6de71df41dbe3bd0dd
confMgmt.out      6130     OK
d8d23d19e7c661ed747e7cb72253506e
diag.out         39189    OK
84fd974dd815bb9800724b3d5581c865
confXML.out       46518    OK
2b80b19745e385e07f9cb629ee63ed60
confObj.out       114704   OK
2d78e7e12373cc3aa4eff91dba086636
clusterApp.out    20288    OK
584bb81b6530855e5b5977748e3b8a3
cdp.out           27675    OK
eb8df8ebb893030c1d0795f17918059d
systemApp.out     63939    OK
c80d2ed7873f35ffbd4637ae33b67066
ipRouter.out      15917    OK
83a8d86985de2e11b891cdd7a216693a
scsiRouter.out    52074    OK
cef3f5dd7caf307b04b90b7fed38fe7d
authServerApp.out 22156    OK
6d60e7c50a33da0ce6717f7138613c22
ui.out            960766    OK
76a773af1e2210be55d82a3747660c58
```


Commands

16

This section describes all the CLI commands related to VLAN. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

show vlan

To view configuration and operational information about the specified virtual LAN, use the `show vlan` command.

Syntax

```
show vlan [id nn] [brief | config]
```

Table 219: Syntax Description

id nn	The ID of the VLAN to be displayed (Optional)
brief	The keyword used to display name, status and ports for each VLAN (Optional)
config	The keyword used to display detailed configuration information for the specified VLAN or all VLANs (Optional)

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

A VLAN is a group of independent devices that communicate as if they are on the same physical LAN segment, but can actually be located anywhere on the network. The storage router dynamically obtains VLAN information from the switch attached to the Gigabit Ethernet interface. Use the `show vlan` command to learn of any VLANs configured on the attached network.

Examples

The following is an example output from the `show vlan` command, followed by example output from the `show vlan config` command for the VLAN ID *101*:

```
show vlan
VLAN  Name      Status  Ports
-----
101   vlanfoo1  active  ge2
102   vlanfoo2  active  ge2

VLAN  Type  MTU  Interfaces
-----
101   enet  1500
102   enet  1500

show vlan id 101 config
vlan 101 name vlanfoo1 mtu 1500
```

show vtp

To display general configuration and status information about the VLAN Trunk Protocol (VTP), use the `show vtp` command.

Syntax

```
show vtp [config | stats]
```

Table 220: Syntax Description

<code>config</code>	The keyword used to display mode and domain information (Optional)
<code>stats</code>	The keyword used to display operational statistics (Optional)

Defaults

None.

Command Modes

Administrator or Monitor.

Usage Guidelines

VTP must be in Transparent mode to configure VLANs. Use the `show vtp` command to view the current VTP configuration.

Examples

The following is an example output from the `show vtp` command, when the storage router is in VTP Client mode:

```
show vtp
Configuration Revision    : 0
Number of existing VLANs : 2
VTP Operating Mode        : Client
VTP Domain Name           : lab1
```

The following is example output from the `show vtp` command, with the storage router in VTP Transparent mode:

```
show vtp
Configuration Revision    : 0
Number of existing VLANs : 2
VTP Operating Mode        : Transparent
VTP Domain Name           :
```

The following is example output from the `show vtp config` command:

```
show vtp config
vtp mode client
vtp domain lab1
```

The following is example output from the **`show vtp stats`** command:

```
show vtp stats
Summary advertisements received    : 3
Subset advertisements received    : 2
Request advertisements received    : 0
Request advertisements transmitted : 5
```

vlan

To configure a VLAN on the SR 2122 storage router, use the `vlan` command. To delete a VLAN, use the `no` form of this command.

Syntax

```
vlan vid [name vname] [mtusize mtusize]
no vlan vid [force]
```

Table 221: Syntax Description

vid	The VLAN identification number. Enter an integer value between 1 and 4095
name vname	The name of the VLAN, which can be up to 32 characters in length. If not specified, the VLAN name becomes the prefix VLAN and the VLAN identification number, left padded to four bytes. For example, VLAN0002, or VLAN0045. (Optional)
mtusize mtusize	The size of the maximum transfer unit, in bytes. nn is an integer between 1500 and 9000. The default MTU is 1500.
force	Keyword that overrides normal protections, allowing the action to be performed. (Optional)

Defaults

The default VLAN name is composed of the prefix VLAN and the VLAN identification number, left padded to four bytes. The default MTU size is **1500**.

Command Modes

Administrator.

Usage Guidelines

In a cluster environment, all VLANs must be created and maintained on the first storage router to join the cluster. If you issue the `vlan` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router currently handling all VLAN functions.

VLANs are cluster-wide configuration items. When configured and copied to the boot configuration file, HA communications propagate the VLAN information to all storage routers in the cluster. A maximum of 16 logical interfaces (VLANs associated with IP addresses) can be configured per physical Gigabit Ethernet interface in the storage router or cluster.

VLAN information can only be configured when the storage router is in VTP Transparent mode. In Transparent mode, received VTP packets are ignored and VLAN configuration information is retrieved from the storage router cluster.

The storage router uses 802.1Q tagging to carry the VLAN information on packets sent and received on the Gigabit Ethernet interface. The 802.1Q tag is a four-byte field inserted between the source MAC address and ether-type fields in the layer 2 header. It consists of a two-byte Tag Protocol Identifier (TPID) field and a two-byte Tag Control Information (TCI) field. The TPID contains the “protocol type” field (0x8100), which identifies the packet as a valid 802.1Q tagged packet. The TCI contains the 12 bit VLAN Identifier (VID) field and a 3 bit User Priority (UP) field.

Use the `vlan` command to configure VLANs locally when the storage router is connected to a switched network that does not support VTP, but does support 802.1Q VLANs.

Examples

The following set of commands places the storage router in VTP Transparent mode and configures a VLAN named *weblan001* on the storage router. The VLAN ID is 45.

```
vtp mode transparent
Jul 30 15:24:02:Vtp:AS_NOTICE :VTP changed to transparent mode
vlan 45 name weblan001
Jul 30 15:25:45:Vtp:AS_NOTICE :VLAN 45 added (name=VLAN0045,
mtu=1500)
```

vtp domain

To assign a VLAN Trunk Protocol (VTP) domain name to the SR 2122 Storage Router, use the `vtp domain` command. VLAN information will not be accepted from a switch in a different domain.

Syntax

```
ntp domain {domainname | none}
```

Table 222: Syntax Description

domainname	The name of the domain to which the storage router belongs
none	The storage router is not assigned to a specific domain. If the storage router is in VTP Client mode, it will assign itself to the first domain from which it receives a VTP message. This is the default.

Defaults

None. The SR 2122 will assign itself to the first domain from which it receives a VTP message.

Command Modes

Administrator.

Usage Guidelines

In a cluster environment, all VLANs must be created and maintained on the first storage router to join the cluster. If you issue the `ntp domain` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router currently handling all VLAN functions.

The VTP domain name applies to all storage routers participating in a cluster. The VTP domain name is a cluster-wide configuration setting. When the VTP domain name is set using the `ntp domain` command and saved to the boot configuration file (via a `save all` or `save system` command), an HA exchange occurs and the VTP domain name becomes active on all storage routers in the cluster.

Examples

The following example sets the VTP domain name to *Lab_Network*:

```
ntp domain Lab_Network
```

vtp mode

To assign the VTP mode in which the SR 2122 Storage Router operates, use the `vtp mode` command.

Syntax

```
vtp mode {client | transparent}
```

Table 223: Syntax Description

client	The storage router will operate in VTP Client mode. The storage router will exchange VTP packets with an externally attached switch to learn about the VLANs which are accessible in the network. This is the default.
transparent	The storage router will operate in VTP Transparent mode. The SR 2122 will not exchange VTP packets and will only learn about VLANs from explicit storage router configuration via the <code>vlan</code> command.

Defaults

Client.

Command Modes

Administrator.

Usage Guidelines

In a cluster environment, all VLANs must be created and maintained on the first storage router to join the cluster. If you issue the `vtp mode` command from another storage router in the cluster, the CLI displays an informational message with the IP address of the storage router that is currently handling all VLAN functions.

VTP operates in either Client or Transparent mode. In Client mode, the storage router exchanges VTP packets with a locally connected switch to learn about the VLANs available in the network. In Transparent mode, VTP packets are ignored and VLAN information is taken directly from the storage router cluster configuration.

When operating a VTP client, the storage router sends a VTP advertisement when one of the following events occurs:

- The Gigabit Ethernet interface on any storage router in the cluster transitions to the up state and a valid domain name has been either configured or previously learned.
- The VTP domain name changes.
- A VTP summary advertisement is received with a higher configuration revision.
- The switch replies to the storage router with a summary advertisement, followed by one or more subset advertisements.

When operating in Transparent mode, the storage router ignores any VTP packets it might receive. VLANs are configured using the GUI, or the CLI `vlan` command. Use Transparent mode when the storage router is connected to a switched network that does not support VTP but does support 802.1Q VLANs.

Examples

The following example places the storage router in VTP Transparent mode:

```
vtp mode transparent
```


Wizard Commands

17

This section describes all the CLI commands related to the usage of the CLI wizards. The `no` form of any command is shown with the primary command entry. Command information includes syntax, defaults, mode, usage guidelines, examples, and related commands.

clear conf

To return certain configuration settings to factory defaults, use the `clear conf` wizard. The `clear conf` wizard prompts the user to enter the Administrator mode password, and then to indicate which settings to restore to factory defaults.

Syntax

```
clear conf
```

This command has no arguments or keywords.

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

The `clear conf` wizard is available only when the storage router is deployed for SCSI routing. If the storage router is deployed for transparent SCSI routing or iSCSI SAN interconnect, use the `clear conf {all | system}` command to return the storage router configuration to factory default settings.

Follow these guidelines when using the `clear conf` wizard:

- Select **apps** to remove all SCSI routing instances but retain system configuration settings. This also erases the cluster name. It does not delete any saved configurations.
- Select **system** to remove all SCSI routing instances and system configuration settings. This does not delete any saved configurations.
- Select **saved** to delete all backup configuration files from disk.
- Select **all** to remove all SCSI routing instances, system configuration settings, and saved configuration files.

The system reboots if you select **apps**, **system**, or **all**.

System configuration settings include:

- Management and HA interface IP addresses
- Domain name servers
- NTP server and time zone information
- SNMP configuration information
- Administrator and Monitor passwords and administrator contact information
- AAA authentication configuration information
- VLAN and VTP configuration information

Deleting system configuration makes the storage router unavailable to Telnet or web-based GUI sessions until the management interface is reconfigured with an IP address via the console interface connection. The log file is also cleared.

Examples

The following example removes all SCSI routing instances from the storage router. The system configuration settings are retained.

```
clear conf
clear conf all admin-password
```

Table 224: Syntax Description

admin-password	The Administrator-mode password.
----------------	----------------------------------

Defaults

None.

Commands Modes

Administrator.

User Guidelines

This command removes all SCSI routing services, system configuration settings, and saved configuration files. The system reboots after this command.

Deleting system configuration makes the SR 2122 unavailable to Telnet or web-based GUI sessions until the management interface is reconfigured via the RS-232 connection.

Examples

The following example returns all configuration setting for the storage router to the factory default settings. The Administrator password is shown as the default, **hp**.

```
clear conf all hp
```

Table 225: clear conf Field Description

Command	Description
config terminal access	Configures management passwords
config terminal ha	Configures the HA interface
setup cluster	Configures the management interface
setup netmgmt	Configures the network management interface
setup scsi	Configures SCSI routing services
setup time	Configures the system date and time

clear conf all

To return all configuration settings to factory defaults, use the `clear conf all` command.

Syntax

```
clear conf all admin_password
```

This command has no arguments or keywords.

Table 226: Syntax Description

<code>admin_password</code>	The password associated with administrative access to the storage router management interface. Enclose the string in quotes. A string value of "" clears the password. The default password is hp.
-----------------------------	--

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

This command removes all SCSI routing services, system configuration settings, and saved configuration files. The system reboots after this command, at which time you must reconfigure the management port.

Deleting system configuration makes the storage router unavailable to Telnet or web-based GUI sessions until the management interface is reconfigured with the IP address via the console interface connection. The log file is also cleared.

Examples

The following example removes all configuration setting for the storage router to the factory default settings. The Administrator password is shown as the default, **hp**.

```
clear conf all hp
```

clear conf system

To return the system configuration settings to factory defaults without using a wizard, use the `clear conf system` command.

Syntax

```
clear conf system admin_password
```

Table 227: Syntax Description

<i>admin_password</i>	The password associated with administrative access to the storage router management interface. Enclose the string in quotes. A string value of "" clears the password. The default password is hp .
-----------------------	--

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

System configuration settings include:

- Management and HA interface IP addresses
- Domain name servers
- NTP server and time zone information
- SNMP configuration information
- Administrator and Monitor passwords, and administrator contact information
- AAA authentication configuration information
- VLAN and VTP configuration information

This command removes only the system configuration settings. The system configuration includes the management port, dns, admin, monitor login, ntp, and snmp. The system reboots after this command, at which time you must reconfigure the management port.

Deleting system configuration makes the storage router unavailable to Telnet or web-based GUI sessions until the management interface is reconfigured with an IP address via the console interface connection. The log file is also cleared.

Examples

The following example removes the system configuration setting for the storage router to the factory default settings. The Administrator password is shown as the default, **hp**.

```
clear conf system hp
```

scsirouter username

To set the username that will be sent in response to an authentication request from an iSCSI initiator use the `scsirouter username` command.

Syntax

```
scsirouter name username string
```

Table 228: Syntax Description

<i>name</i>	The name of the SCSI routing services instance
<i>username string</i>	User name to associate with the named SCSI routing instance
<i>none</i>	Delete configured user name

Defaults

None.

Command Modes

Administrator.

Usage Guidelines

Use the `scsirouter username` command to set the user name sent in the response to an authentication request from an iSCSI initiator. If no user name is configured, an empty string will be sent in the response.

Example

The following example sets the user name for the SCSI routing instance named *foo* to *bob*:

```
[HP SR2122-2]# scsirouter foo username bob
```

The following example deletes the user name for the SCSI routing instance named *foo*.

```
[HP SR2122-2]# scsirouter foo username none
```

setup

To configure the storage router using the initial configuration wizards in sequence, use the `setup` command. The wizard prompts the user through the initial configuration steps.

Syntax

```
setup
```

This command has no arguments or keywords.

Defaults

For multiple-choice questions, the system presents the choices in brackets []. Each multiple-choice question has a default answer that is selected when you press **Enter** or **Return**. The default is shown in parenthesis (). For example:

```
Enable High Availability? [yes/no (no)]
```

For configuration variables, the current value saved in the system is presented in brackets. For example, when configuring a SCSI routing instance server interface:

```
Network mask? [255.255.255.0]
```


If the configuration variable does not have a value, the system presents a set of “empty” brackets [(empty)] or a template that provides the expected format of the value. For example:

```
system name? [(empty)]
```

Command Modes

Administrator.

Usage Guidelines

Initial system configuration and subsequent reconfiguration can be performed via interactive configuration wizards, either through the console interface or via Telnet (once the management interface has been configured). The configuration wizards prompt you for the necessary information to accomplish the specific configuration task and may invoke multiple commands to compile their functions.

The CLI provides the following configuration wizards:

- **Setup** runs all the individual setup command utilities in sequence.
- **Management interface** configures the management interface with a system name, IP address, and optional DNS server information.
- **Date and Time** configures the time zone, use (or non-use) of daylight savings time, the current date and time, and the NTP server address (if one is present).
- **Network Management** configures the user of Telnet, web-based GUI, and SNMP for managing the storage router over the network.
- **Management Access** configures passwords for monitoring and configuring the storage router.
- **SCSI routing** configures the use of the SR 2122 SCSI routing capabilities. This wizard is only available when the storage router is deployed for SCSI routing; it is not available if the storage router is deployed for transparent SCSI routing or iSCSI SAN interconnect.

For storage routers deployed for SCSI routing, the CLI also provides a Cluster wizard that configures the storage router to participate in a high-availability cluster. The initial configuration script configures the storage router’s high-availability environment, so **setup** does not run the Cluster wizard. The `setup cluster` command can be run after initial system configuration to change the storage router’s configuration mode from standalone to clustered, to change membership from one cluster to another, or to resign from a cluster and run as a standalone storage router.

During configuration with the setup wizard, operational changes take place and are applied to the system currently running. For example, after the Network Management wizard completes, SNMP network management will be configured for the storage router. However, these changes are not saved to the system boot configuration until the end of the last configuration utility. To quit a configuration wizard without saving the changes, press **Ctrl-C** at any time before the end of the wizard, and then reboot the storage router to restore previous values.

Some changes may be retained after a reboot. Be sure to review the prompts that display during configuration using setup command utilities.

After entering the setup command wizard, several informational messages display, including the following prompt:

```
User level for setup? [novice/expert (expert)]
```

- Enter `novice` to continue with the configuration process. Help text displays for each setup command utility.
- Enter `expert` to continue with the configuration process, suppressing all help text. If you are an experienced user, familiar with the setup command utility, you may prefer this option.

At the end of wizards, the following prompt displays:

```
Done with setup.
```

Examples

The following example shows the initial system response to the setup command:

```
setup
```

```
You are about to set up the SR 2122. Running this wizard will modify  
the configuration of this system.
```

During setup, operational changes will take place. However, these changes are not saved until the end of the script. To quit the setup

wizard without saving changes, **** hit CTRL-C at any time ****. Reboot to restore previous values.

For multiple choice questions, the system will present the choices enclosed in brackets []. Each multiple choice question has a default answer that is selected when you press return.

Example: [yes/no (no)].

Choices are yes and no. No is the default answer.

For configuration variables, the current value saved in the system is presented in brackets [varname]. If the configuration variable does not have a value, the system will present a set of brackets [(empty)] or a template that provides the expected format of the value.

Example: [mySR2122] configuration variable has a value

Example: [(empty)] configuration variable does not have a value, no template

Example: [A.B.C.D] template for an IP address.

User level for setup? [novice/expert (expert)]

setup access

To configure passwords for monitoring and administering the storage router and setting administrative contact information, use the **setup access** wizard. The wizard prompts the user to enter and confirm new passwords.

Syntax

```
setup access
```

This command has no arguments or keywords.

Defaults

The factory default password for both Administrator mode and Monitor mode is **hp**.

Command Modes

Administrator.

Usage Guidelines

The wizard prompts the user to enter (and confirm by re-entering) the new Monitor password, which allows view-only storage router access. The user is also prompted to enter (and confirm by re-entering) the new Administrator password, which allows changes to be made to the storage router configuration. If the new password is incorrect, a “try again message” is displayed.

The last prompt asks if you want to change the administrative contact information. If yes, you are prompted for the following: administrator name, phone, pager, and email information.

Examples

The following examples set the Monitor mode and Administrator mode passwords for the storage router, but does not apply them to the console interface. Administrator contact information is also configured. Note that passwords display as asterisks when entered.

```
setup access
#####
## Management Access Setup ##
#####
```

The SR2122CLI and GUI are protected by two passwords. The initial password entered when logging in allows the user to monitor the SR2122, but does not allow changes. The "admin" password allows the user to make configuration changes.

**** Password Rules ****

A password can contain any combination of characters excluding those specifically called out in the CLI specification. The password should not be something familiar to you and not be easy to guess.

```
Enter the new "monitor" password: *****
Enter the new "monitor" password again: *****
Enter the new "admin" password: *****
Enter the new "admin" password again: *****
```

The new passwords will apply to all telnet and web-based GUI sessions. They will also be applied to the console. If the SR2122 console is in a physically secure location, console passwords are not recommended since they can be lost or forgotten. If the SR2122 is deployed in a less secure environment, the passwords should be applied. If passwords are subsequently lost, contact HP Technical Support for information on recovery.

```
Apply passwords to console? [yes/no (no)] no
```

The administrative contact is the person or group responsible for configuration and management of the SR2122. The system will store a name, e-mail address, phone number, and pager number for the system administrator. Management applications can retrieve this

information and provide it to a support person or directly use it to e-mail or page the administrator.

```
Input Administrator Info? [yes/no (yes)] yes
Administrator name? [(empty)] Bob
Phone? [(empty)] (952) 123-4567
Pager number? [(empty)] (952) 123-4467
Email? [(empty)] bob@mycomp.com
```

Done with setup.

setup cluster

To configure the high-availability environment for the storage router or to add the storage router to a cluster or remove it from an existing cluster, use the **setup cluster** wizard. The wizard prompts the user to select the appropriate HA configuration mode, enter a cluster name, and (if necessary) HA interface IP address and subnet mask.

Syntax

```
setup cluster
```

This command has no arguments or keywords.

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the allowable responses are *merge* and *delete*, and the default is **delete**.

```
Retain or delete applications? [retain/delete (delete)]
```

Command Modes

Administrator.

Usage Guidelines

The high-availability (HA) features of the SR 2122 Storage Router are designed around a cluster of systems that back each other up in case of failure. A cluster consists of up to four identically configured storage routers that continually exchange HA information over their HA and management interfaces.

Clusters are defined by name. The `setup cluster` command prompts the user for the appropriate HA configuration mode and the cluster name.

- Use the **standalone** keyword to identify a storage router that will not participate in a storage router cluster. A stand alone storage router does not require the management or HA interfaces to be available in order to complete the system configuration. The MGMT and HA ports do not need to be cabled.
- Use **clustered** keyword to identify a storage router that will participate in a storage router cluster. A clustered storage router requires the management and HA interfaces to be available in order to complete the system configuration. The MGMT and HA ports must be correctly cabled. If clustered, the user is also prompted for the **HA IP address** if none is currently assigned.

This command also prompts the user to either retain this storage router's configuration, merging it with others in the cluster, or to delete this storage router's application configuration data (SCSI running instances and cluster configuration information) and replace it with cluster data. Retained data is replicated to other storage routers in the cluster. When joining the existing cluster, access list information is always deleted and replaced by the cluster's accesslist information.

Retaining configuration data could provide unexpected results.

Changing the storage router's cluster name, thereby joining another cluster, has the following effects on its existing configurations and operations:

- All SCSI routing instances are failed-over to another member in the original cluster.
- All applications are stopped.
- The cluster name is changed.
- If the user has chosen to retain data, any unsaved cluster configuration information is saved.
- The system reboots. Configuration information is exchanged. All of the original SCSI routing instances appear in the new cluster, unless the user has chosen to delete rather than retain data.

- Access lists are always deleted. To preserve an existing access list and make it available to the new cluster, the user must save the access list to a configuration file before issuing the `setup cluster` command. Make the saved configuration file available to the storage router currently performing access list maintenance functions for the cluster (via the `copy` command), and then restore the saved access list to the new cluster from that configuration file.
- For cases in which the names of SCSI routing instances are duplicated within the new cluster (meaning instances of the same name are already running in the new cluster), configuration data from the old cluster is deleted in favor of what is currently running in the new cluster.

Examples

The following examples shows the initial system response to the `setup cluster` command:

```
setup cluster
```

```
The system has the ability to run in a standalone or clustered
state. By default, the system will run in a clustered state and
communicate with other SR2122s in the same cluster. A single SR2122
is deployed and you don't intend to add a second SR2122 to provide
high availability features in a clustered configuration, you should
configure the SR2122 in standalone mode. Enter CTRL-C at any prompt
to cancel changes and return to the command prompt.
```

```
HA configuration? [standalone/clustered (standalone)] clustered
```

```
If you select HA configuration mode clustered, the wizard prompts
you to enter an HA IP address:
```

```
To determine the health of other SR2122s in a cluster, the SR2122
must send occasional heartbeat packets on at least two interfaces
(in case one interface has problems). By default, the interfaces
used are the 10/100 management interface (already set up) and the
10/100 HA interface. Please select an IP address and network mask
for the HA interface.
```

```
HA Interface IP address? [A.B.C.D/nn] 10.1.2.10/24
```

```
After selecting the HA configuration mode, and optionally setting
the HA IP address, the wizard prompts you to enter a cluster name:
```

```
When you change the cluster that the SR2122 belongs to, you need to
decide if you want the applications running on the SR2122 to be
```


deleted or if you want them to be retained and merged with the new cluster.

Change cluster to? [3d000120]

For a change from standalone to clustered:

If you retain the configuration, there may be conflicts when the applications are replicated between this SR2122 and others in the new cluster.

For a change from clustered to standalone:

You can retain the configuration without causing any scsirouter instance conflicts for this SR2122 since it will be the only member of the new cluster.

Retain or delete applications? [retain/delete (delete)] **retain**

If you choose to retain the storage router configuration, an additional warning displays:

```
#####  
Please confirm that you want to retain the configuration.  
#####
```

All configuration settings will be saved. The system will REBOOT if you answer "yes"

** Enter CTRL-C to cancel. **

Are you sure you want to retain the configuration? [must type "yes"] **yes**

If you choose to delete your existing configuration, this warning displays:

```
#####  
Please confirm that you want to delete the configuration.  
#####
```

Cluster configuration settings will be saved. The system will REBOOT if you answer "yes"

** Enter CTRL-C to cancel and abort the cluster change. **

Are you sure you want to delete the configuration? [must type "yes"]

After confirming your selection, the storage router automatically reboots.

setup mgmt

To configure the storage router management interface, use the **setup mgmt** wizard. The wizard prompts the user to enter the storage router system name, management interface IP address and subnet mask, optional default gateway, and DNS information.

Syntax

```
setup mgmt
```

This command has no arguments or keywords.

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current storage router system name is *SR2122_lab1*:

```
SR2122system name? (SR2122_lab1)
```

Command Modes

Administrator.

Usage Guidelines

The management interface must be configured before the Telnet interface or web-based GUI can be used for configuration or monitoring tasks. When the wizard is completed, the system displays notification that the management interface is operational. The user may be prompted to reboot the storage router at this time. To continue configuration via a Telnet session, a reboot is required.

Examples

The following shows the initial system response to the `setup mgmt` command:

```
setup mgmt
```

```
#####
## Management Interface Setup ##
#####
```

Please choose a name for the SR2122. This name is associated with the SR2122 Management Interface IP address. If you wish to enable network management on the SR2122, you should add the system name you provide at this prompt and its IP address to a domain name server (nis, nis+, WINS).

```
SR2122system name? [stimpy]
```

The SR2122 may be managed using telnet, or a web-based GUI, or SNMP via the 10/100 Ethernet interface labeled "mgmt" on the front panel of the system. This interface must be assigned an IP address.

```
Management Interface IP address? [10.82.1.40/24]
```

If the SR2122 is to be managed from a subnet other than the one to which it is physically attached, a static route is required. The static route format is "destination/netmask gateway".

```
Static route for Management Interface? [0.0.0.0/0 10.82.1.1]
```

If IP addresses are to be entered as host names via any of the SR2122 management interfaces, a Domain Name Server must be specified. A secondary DNS may be specified for use if the primary DNS is not available.

```
Primary DNS Server? [A.B.C.D]
```

```
Setting up the management interface ...Done
```

The management port is now operational. It may be tested using ping or telnet from a host on the network.

```
Done with setup.
```

setup netmgmt

To enable network management via any or all of the available interfaces (Telnet, web-based GUI, or SNMP), use the `setup netmgmt` wizard. The wizard prompts the user to selectively enable the various interfaces and, if SNMP is enabled, prompts the user to enter the read and write community information, IP addresses for SNMP traps, and additional SNMP configuration information.

Syntax

```
setup netmgmt
```

This command has no arguments or keywords.

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets.

Command Modes

Administrator.

Usage Guidelines

All network management interfaces are enabled by default, with SNMP “GETS” via the public read community. Run this wizard to disable any of these interfaces or to change the SNMP read community, configure the SNMP write community for SNMP “sets,” or add addresses for SNMP traps.

Examples

The following example shows the initial system setup response to the `setup netmgmt` command:

```
setup netmgmt
#####
## Network Management Access Setup ##
#####
This wizard will enable you to configure access to telnet, the
web-based GUI, and configure SNMP. By default, telnet and the
web-based GUI are enabled. SNMP gets via the "public" community are
also enabled via the 10/100 management interface. If you want to
change these values or configure other SNMP features, please set up
the network management.

Set up Network Management? [yes/no (yes)]
Enable telnet on all interfaces? [yes/no (yes)]
Configure SNMP? [yes/no (yes)]
Read Community? [public]
Write Community? [private]
First IP address for SNMP traps? [A.B.C.D]
Network Management setup is complete.
```

By default, these methods of network management will work from any network which is not separated from the SR2122 by a firewall or other traffic-limiting device. To further specify security requirements, please use the normal configuration functions of the CLI or GUI after completing this wizard.

Done with setup.

setup scsi

To configure an initial SCSI routing instance for the storage router, use the **setup scsi** wizard. The wizard prompts the user to enter the name of the SCSI routing instance (maximum 32 characters), configures the Gigabit Ethernet and Fibre Channel interfaces, and discovers all Fibre Channel devices connected to the storage router. More granular configuration OS SCSI routing instances can be performed via the CLI or the web-based GUI.

Syntax

```
setup scsi
```

This command has no arguments or keywords.

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets.

Command Modes

Administrator.

Usage Guidelines

After the wizard finishes the discovery process, it displays a default mapping of target names with all accessible storage devices. Target names can be modified using the web-based GUI or CLI commands.

The `setup scsi` command can only be run at initial system configuration or when no SCSI routing instance is currently configured on the storage router.

Examples

The following example shows the initial system response to the `setup scsi` command:

```
setup scsi
scsirouter instance name? [(empty)] dino
The scsirouter instance communicates with iSCSI hosts via the
gigabit ethernet interface. To enable communication, you need to
assign an IP address and network mask to the scsirouter instance
for it to use on the gigabit ethernet interface.
```

```
IP Address? [0.0.0.0/24] 10.1.28.9/24
```

```
Now discovering all FC devices connected to the SR2122...
```

A default mapping of target names with all accessible FC devices has been created and is shown in the table below. The default names

for the targets can be edited using the "add scsirouter" command or on the Configuration screen via the GUI.

Interface	lunwwn	wwpn	portId	lun	vendor	product	serial
-----	-----	-----	-----	-----	-----	-----	-----
fc2	20201912cc	2103912cc	0x102e2	0	DEC	HSG80	
	3CC05670S6DNTE						
fc2	2007c52f42	210072f42	0x102e4	0	DEC	HSG80	
	3CC05800S6DDTE						
fc2	2000c588d2	2100588d2	0x102e8	0	DEC	HSG80	
	3CC056N116DVCY						
fc2	2007c59d28	210c59d28	0x102e1	0	DEC	HSG80	
	3CC0007116DSRB						

scsirouter setup is complete.
Done with setup.

setup time

To set current date and time information and other time-related configuration setting use the **setup time** wizard. The storage router uses date and time information for log files and the user interface.

Syntax

```
setup time
```

This command has no arguments or keywords.

Defaults

Defaults or current values are shown in parentheses within the allowable response brackets. In the following example, the current date is 11/16/2001:

```
Date (mm/dd/yyyy)? [11/16/2001]
```

Command Modes

Administrator.

Usage Guidelines

The wizard prompts the user to enter the appropriate time zone (as an offset from Universal/GMT). The user can also enter an optional name or IP address of an NTP server, to be used by the SR 2122 for date and time synchronization. Finally, the wizard prompts for the current date and time if no NTP server address is provided.

Examples

The following example shows the initial system response to the `setup time` command:

```
setup time
```

```
To provide correct information in log files and user interfaces,
the SR2122 must have a reasonably accurate date and time. To use
Daylight Savings Time or specify time zone by geographic region use
the "clock timezone" command.
```

```
The time zone must be entered as an offset from GMT.
```

```
0=[0000 GMT]      1=[-0100 WAT]    2=[-0200 AT]
3=[-0300 Brazil]  4=[-0400 AST]    5=[-0500 EST]
6=[-0600 CST]     7=[-0700 MST]    8=[-0800 PST]
9=[-0900 YST]     10=[-1000 AHST]  11=[-1100 NT]
12=[+1200 IDLW]   13=[+1100 WST]   14=[+1000 GST]
15=[+0900 JST]    16=[+0800 CCT]   17=[+0700 WAST]
18=[+0600 ZP6]    19=[+0500 ZP5]   20=[+0400 ZP4]
21=[+0300 BT]     22=[+0200 EET]   23=[+0100 CET]
Time Zone? [0-24] 6
```

```
Follow daylight savings time? [yes/no] yes
```

```
If a Network Time Protocol (NTP) server is in use on a network
reachable via the SR2122 management interface, it may be used to
keep the SR2122 date and time in sync with the rest of the network.
```

```
NTP server IP address? [0.0.0.0] 10.1.9.2
Date? [dd/mm/yyyy] 07/27/2000
Time? [hh:mm:ss] 12:00:00
```

```
Date and time are now configured.
```


Regulatory Compliance Notices



Regulatory Compliance Identification Numbers

For the purpose of regulatory compliance certifications and identification, your product has been assigned a unique HP Series Number. The series number can be found on the product label, along with the required approval markings and information. When requesting compliance information for this product, always refer to this series number. The series number should not be confused with the marketing name or model number of the product.

Federal Communications Commission Notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

The rating label on the device shows the classification (A or B) of the equipment. Class B devices have an FCC logo or FCC ID on the label. Class A devices do not have an FCC logo or FCC ID on the label. After the Class of the device is determined, refer to the corresponding statement in the following sections.

Class A Equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit that is different from that to which the receiver is connected
- Consult the dealer or an experienced radio or television technician for help

Declaration of Conformity for Products Marked with the FCC Logo, United States Only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding your product, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
P. O. Box 692000, Mail Stop 530113
Houston, Texas 77269-2000
- 1-800-652-6672 (1-800-OK COMPAQ) (For continuous quality improvement, calls may be recorded or monitored.)

For questions regarding this FCC declaration, contact us by mail or telephone:

- Hewlett-Packard Computer Corporation
P. O. Box 692000, Mail Stop 510101
Houston, Texas 77269-2000
- 1-281-514-3333

To identify this product, refer to the part, series, or model number found on the product.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Computer Corporation may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Power Cords

The power cord set included in your server meets the requirements for use in the country where you purchased your server. If you need to use this server in another country, you should purchase a power cord that is approved for use in that country.

The power cord must be rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cord should be greater than the voltage and current rating marked on the product. In addition, the cross sectional area of the wire must be a minimum of 1.00 mm² or 18AWG, and the length of the cord must be between 6 feet (1.8 m) and 12 feet (3.6 m). If you have questions about the type of power cord to use, contact your HP authorized service provider.

A power cord should be routed so that it is not likely to be walked on or pinched by items placed upon it or against it. Particular attention should be paid to the plug, electrical outlet, and the point where the cord exits from the product.

Mouse Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Notice (Avis Canadien)

Class A Equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B Equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union Notice

Products with the CE Marking comply with both the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (the equivalent international standards are in parenthesis):

- EN55022 (CISPR 22) – Electromagnetic Interference
- EN55024 (IEC61000-4-2, 3, 4, 5, 6, 8, 11) – Electromagnetic Immunity
- EN61000-3-2 (IEC61000-3-2) – Power Line Harmonics
- EN61000-3-3 (IEC61000-3-3) – Power Line Flicker
- EN60950 (IEC950) – Product Safety

Japanese Notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文をお読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwanese Notice

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Laser Device

All HP systems equipped with a laser device comply with safety standards, including International Electrotechnical Commission (IEC) 825. With specific regard to the laser, the equipment complies with laser product performance standards set by government agencies as a Class 1 laser product. The product does not emit hazardous light; the beam is totally enclosed during all modes of customer operation and maintenance.

Laser Safety Warnings



WARNING: To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
 - Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
 - Allow only HP authorized service technicians to repair the laser device.
-

Compliance with CDRH Regulations

The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

Compliance with International Regulations

All HP systems equipped with laser devices comply with appropriate safety standards including IEC 825.

Laser Product Label

The following label or equivalent is located on the surface of the HP supplied laser device.



This label indicates that the product is classified as a CLASS 1 LASER PRODUCT. This label appears on a laser device installed in your product.

Laser Information

Table 229: Laser Information

Feature	Description
Laser type	Semiconductor GaAlAs
Wave length	780 nm +/- 35 nm
Divergence angle	53.5 degrees +/- 0.5 degrees
Output power	Less than 0.2 mW or 10,869 W m ⁻² sr ⁻¹
Polarization	Circular 0.25
Numerical aperture	0.45 inches +/- 0.04 inches

Electrostatic Discharge

B

To avoid damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding Methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm \pm 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have a HP authorized reseller install the part.

Note: For more information on static electricity, or assistance with product installation, contact your HP authorized reseller.

/Bits 1

A

- aaa authentication enable 7
- aaa authentication iscsi 9
- aaa authentication login 12
- aaa generate password 14
- aaa group server radius 15
- aaa group server tacacs+ 16
- aaa new-model 17
- aaa test authentication 18
- aaa test authentication cancel 19
- access lists
 - associating with iSCSI target 330
- accesslist 269
- accesslist description 272
- adding
 - iSCSI target description 337
 - iSCSI targets 353
- admin contactinfo 42
- admin password 43
- Administrative Commands 4, 41
- administrator contact information 42
- authorized reseller, HP xvi

B

- Basic Monitor Commands 3
- boot straps, using 466
- bootconfig 1

C

- Canadian Notice (Avis Canadien) 460
- CDB retry count 306
- CDP Commands 85
 - cdp enable 86
 - cdp holdtime 87
 - cdp interface 88
 - cdp timer 89
- CDRH 462
- Center for Devices and Radiological Health See CDRH
- clear conf 434
- clear conf all 437
- clear conf system 438
- clear counters fcip 194
- clear counters fcip command 194
- clear counters fc-server 158
- clear counters interface 195
- clear counters scsirouter 273
- clear log 240
- clear scsirouter failover 176
- clear scsirouter primary 196
- clear scsirouter primary command 196
- clear static 274
- clear static command 274
- clearing
 - accumulated operational statistics 194
 - designated primary for SCSI routing instance 196
 - static mappings for transparent SCSI routing 274
- Clock Commands 101

- clock set [102](#)
- clock timezone [103](#)
- Compaq series number [457](#)
- Configuration Commands [107](#)
- Conventions [xii](#)
- conventions
 - document [xii](#)
 - equipment symbols [xiii](#)
 - text symbols [xii](#)
- copy http [402](#)
- copy ftp [403](#)
- creating
 - FCIP instances [287](#)

D

- debug aaa [20](#)
- debug fcip [276](#)
- debug fcip command [276](#)
- debug ip rip [197](#)
- debug ip rip command [197](#)
- debug isns [199](#)
- debug isns command [199](#)
- debug scsirouter [278](#)
- debug scsirouter iscsitrace [201](#)
- debug scsirouter iscsitrace command [201](#)
- debug scsirouter target [279](#)
- Declaration of Conformity [459](#)
- Defaults [327](#)
- Definitions [1](#)
- delete accesslist [280](#)
- delete fcip [283](#)
- delete fcip command [283](#)
- delete fc-server [159](#)
- delete savedconfig [108](#)
- delete script [45](#)
- delete scsirouter [284](#)
- delete software version [405](#)
- deleting
 - FCIP instance elements [283](#)
 - FCIP instances [283](#)
 - saved configuration files [108](#)

- disabling
 - FCIP instances [298](#)
- document
 - conventions [xii](#)
- download software [406](#)

E

- electrostatic discharge See ESD
- enable [46](#)
 - connections [338](#)
 - FCIP instances [298](#)
 - SLP for SCSI routing instance [327](#)
- equipment symbols [xiii](#)
- ESD (electrostatic discharge)
 - obtaining additional information [466](#)
 - precautions [465](#)
 - preventing [465](#)
 - storing products [465](#)
 - transporting products [465](#)
 - types of damage from [465](#)
- European Union Notice [461](#)
- exit [46](#)

F

- failover scsirouter [177](#)
- FC [1](#)
- FC interfaces
 - displaying
 - debug information [143](#)
- FCC notices
 - Class A Equipment [458](#)
 - Class B Equipment [458](#)
 - classification label [457](#)
 - Declaration of Conformity [459](#)
 - device modifications [459](#)
 - mouse [460](#)
- FCIP
 - assigning protocol (raw or TCP/IP) [293](#), [295](#)
 - clear counters [194](#)
 - creating instance [287](#)
 - debugging [276](#)

- deleting instance [283](#)
- displaying
 - troubleshooting information [373](#)
- enable trace facilities [276](#)
- reset operational statistics [194](#)
- restoring instance [303](#)
- saving configuration [305](#)
- selecting connection protocol operational parameters [289](#)
- setup wizard [362](#)
- sharing a network interface [301](#)
- starting instance [298](#)
- stopping instance [298](#)
- fcip [287](#)
- fcip command [287](#)
- fcip destination config [289](#)
- fcip destination config command [289](#)
- fcip destination tcpclient [293](#)
- fcip destination tcpclient command [293](#)
- fcip destination tcpserver [295](#)
- fcip destination tcpserver command [295](#)
- fcip enable [298](#)
- fcip enable command [298](#)
- fcip networkif [299](#)
- fcip networkif command [299](#)
- fc-server autoconfig [160](#)
- fc-server description [163](#)
- fc-server enable [164](#)
- fc-server server [165](#)
- fc-server serverif [166](#)
- Federal Communications Commission notices
 - See FCC notices
- Federal Communications Commission Notice [457](#)
- Fibre Channel Port Commands [137](#)
- Fibre Channel Server Commands [157](#)
- FibreChannel [1](#)

G

- GbE [1](#)
- Getting Help [xv](#)
- getting help [xv](#)
- Gigabit Ethernet [1](#)
- Gigabit Ethernet interfaces
 - configuring for SCSI routing [323](#)
 - packet tracing [228](#)
 - troubleshooting [228](#)
- grounding methods [466](#)
- Grounding Methods [466](#)
- grounding straps
 - specifications [466](#)
 - wearing [466](#)
- grounding, suggested equipment for [466](#)

H

- HA [1](#)
- HA Commands [175](#)
- halt [48](#)
- heel straps, using [466](#)
- help [49](#)
- help, obtaining [xv](#)
- High Availability [1](#)
- hostname [50](#)
- HP
 - authorized reseller [xvi](#)
 - storage website [xv](#)
 - technical support [xv](#)

I

- interface fc? topology [137](#), [140](#)
- interface fci? mode [137](#)
- interface fci? mode command [137](#)
- interface ge? [203](#)
- interface ge? ip-address [205](#)
- interface ha [178](#)
- interface ha command [178](#)
- interface ha ip-address [206](#)
- interface mgmt [207](#)
- interface mgmt command [207](#)

interface mgmt ip-address [209](#)

interfaces

 configuring

 HA [178](#)

 management [207](#)

Introduction [1](#)

IP Commands [193](#)

ip default-gateway [210](#)

ip domain-name [211](#)

ip name-server [212](#)

IP packet trace [228](#)

ip radius source-interface [21](#)

ip route [213](#)

ip tacacs source-interface [22](#)

iSCSI

 configuring use of CRC [333](#)

 targets

 allowing connections [339](#)

 configuring [343](#), [347](#), [353](#)

 disabling [339](#)

 enabling [339](#)

iSNS

 display configuration [232](#)

 display operational statistics [232](#)

 enabling communications [215](#)

 TCP protocol [215](#)

 troubleshooting [199](#), [226](#)

 UDP protocol [215](#)

isns enable [215](#)

isns enable command [215](#)

isns refresh [217](#)

J

Japanese Notice [461](#)

L

laser device

 product classification label [463](#)

 radiation warning [462](#)

 regulatory compliance notice [462](#)

Laser Device [462](#)

logging [242](#)

Logging Commands [239](#)

logging on [243](#)

logging syslog [241](#)

logout [51](#)

M

MAC [1](#)

management interface

 configuring [207](#)

Media Access Control [1](#)

monitor password [52](#)

mouse compliance statement [460](#)

Mouse Compliance Statement [460](#)

N

no debug fcip command [276](#)

no debug ip rip command [197](#)

no debug isns command [199](#)

no debug scsirouter iscsitrace command [201](#)

no fcip enable command [298](#)

no isns enable command [215](#)

no scsirouter slp enable command [327](#)

no scsirouter target enable command [338](#)

ntp peer [104](#)

P

packet tracing [228](#)

parts

 proper handling [465](#)

 storing [465](#)

 transporting [465](#)

passwords

 about [319](#)

 configuring

 for authentication [319](#)

 encrypted format [320](#)

 rules [319](#)

ping [218](#)

R

- Rack Stability [xiv](#)
- rack stability, warning [xiv](#)
- radius-server deadtime [23](#)
- radius-server host [24](#)
- radius-server key [27](#)
- radius-server retransmit [28](#)
- radius-server timeout [29](#)
- read [53](#)
- read-only access to storage
 - restrictions on [330](#)
- reboot [56](#)
- Regulatory Compliance Identification Numbers [457](#)
- regulatory compliance notices
 - Canadian [460](#)
 - Class A equipment [458](#)
 - Class B equipment [458](#)
 - Compaq series number [457](#)
 - device modifications [459](#)
 - European Union [461](#)
 - identification number [457](#)
 - Japanese [461](#)
 - laser devices [462](#)
 - mouse compliance statement [460](#)
 - Taiwanese [462](#)
- Reserved Words [3](#)
- restore aaa [109](#)
- restore accesslist [110](#)
- restore all [111](#)
- restore fcip [303](#)
- restore fcip command [303](#)
- restore scsirouter [113](#)
- restore system [114](#)
- restore vlan [116](#)
- restoring
 - FCIP instance [303](#)
- restrict [220](#)
- restrict console [219](#)
- RIP
 - troubleshooting [197](#)
- runningconfig [2](#)

S

- save aaa [117](#)
- save accesslist [119](#)
- save all [120](#)
- save fcip [305](#)
- save fcip command [305](#)
- save fc-server [122](#)
- save scsirouter [123](#)
- save system [124](#)
- save vlan [125](#)
- savedconfig [2](#)
- saving
 - FCIP instance configuration [305](#)
- SCSI Commands [247](#)
- SCSI Router Commands [269](#)
- SCSI routing instances
 - adding iSCSI target description [337](#)
 - allowing connections to iSCSI target [339](#)
 - assigning preferred storage router [322](#)
 - assigning primary storage router [321](#)
 - associating access lists with targets [329](#)
 - configuring
 - CDB retry count [306](#)
 - primary [196](#)
 - server interfaces [323](#)
 - use of iSCSI CRC [333](#)
 - disabling
 - connections [338](#)
 - iSCSI targets [339](#)
 - enabling
 - connections [338](#)
 - iSCSI targets [339](#)
 - SLP [327](#)
 - failover list [313](#)
 - mapping targets [342, 346, 349, 352](#)
 - maximum outstanding commands per session [356](#)
 - password for iSCSI authentication [318](#)
 - sending LUN reset [316](#)
 - troubleshooting
 - connections [201](#)
 - user name for iSCSI authentication [360](#)

- scsirouter 289, 308
- scsirouter authentication 30, 309
- scsirouter cdbretrycount 306
- scsirouter cdbretrycount command 306
- scsirouter client authenticate 161, 310
- scsirouter description 311
- scsirouter enable 312
- scsirouter failover 178, 180, 313
- scsirouter failover command 313
- scsirouter lun reset 248, 316
- scsirouter lun reset command 316
- scsirouter password 182, 185, 318
- scsirouter password command 318
- scsirouter primary 183, 321
- scsirouter primary command 321
- scsirouter reserveproxy 249
- scsirouter serverif 224, 323
- scsirouter serverif command 323
- scsirouter slp enable 327
- scsirouter slp enable command 327
- scsirouter target {enabled | disabled} 253
- scsirouter target {lunid | serial | wwpn} #? 342
- scsirouter target {lunid | serial | wwpn} #?
command 342
- scsirouter target {lunid | serial | wwpn} #? 342
- scsirouter target {serial | lunwwn | wwpn} #?
255
- scsirouter target accesslist 250, 329
- scsirouter target accesslist command 329
- scsirouter target crc 333
- scsirouter target crc command 333
- scsirouter target description 252, 336
- scsirouter target description command 336
- scsirouter target enable 338
- scsirouter target enable command 338
- scsirouter target lun lunid 346
- scsirouter target lun lunid command 346
- scsirouter target lun lunwwn 260
- scsirouter target lun serial 258, 349
- scsirouter target lun serial command 349
- scsirouter target lun targetid 262
- scsirouter target lun wwnn 346
- scsirouter target lun wwpn lun 263
- scsirouter target lun wwpn lun command 352
- scsirouter target maxcmdqueuedepth 356
- scsirouter target maxcmdqueuedepth command
356
- scsirouter target profile 265
- scsirouter target trespass 358
- scsirouter target trespass command 358
- scsirouter target wwpn 266
- scsirouter username 360, 439
- scsirouter username command 360
- series number for regulatory compliance 457
- server interface
 - configuring for FCIP instance 300
 - configuring for SCSI routing instance 325
- setup 440
- setup access 443
- setup cluster 446
- setup fcip 362
- setup fcip command 362
- setup mgmt 450
- setup netmgmt 452
- setup scsi 453
- setup time 455
- show aaa 31
- show accesslist 365
- show admin 57
- show boot 127
- show bootconfig 128
- show buffers 58
- show cdp 90
- show cdp entry 91
- show cdp interface 92
- show cdp neighbors 94
- show cdp traffic 98
- show cli 64
- show clock 105
- show cluster 185
- show cpu 65
- show crash 66
- show debug fc? 141
- show debug fcip 373

- show debug fcip command 373
- show debug fc-server 168
- show debug interface command 228
- show debug interface fc? 143
- show debug interface fc? command 143
- show debug interface ge? 228
- show debug isns 226
- show debug isns command 226
- show debug scsirouter 367
- show devices 143, 145
- show diagnostics 67
- show fc-server 170
- show ha 187
- show hosts 148
- show interface 150
- show ip 230
- show isns 232
- show isns command 232
- show logging 244
- show memory 68
- show modules 69
- show restrict 71
- show route 237
- show runningconfig 133
- show savedconfig 135
- show script 72
- show scsirouter 375
- show sessions 74
- show slp command 381
- show snmp 396
- show software version 408
- show stack 75
- show static command 383
- show system 77
- show task 79
- show tech-support 82
- show version 409
- show vlan 424
- show vtp 425
- SLP
 - discovering
 - all registered services 389
 - attributes 385
 - displaying status 381
 - enabling for SCSI routing instances 327
- slp findattr 385
- slp findattr command 385
- slp findsrvtypes 389
- slp findsrvtypes command 389
- SNMP Commands 395
- snmp-server 397
- software http url 410
- software http username 411
- Software Management Commands 401
- software proxy 412
- software proxy url 413
- software proxy username 415
- software tftp 416
- software version 417
- Special Keys 2
- starting
 - FCIP instances 298
- static iscsibinding interface autolearn 390
- static iscsibinding interface autolearn command 390
- static iscsibinding interface command 392
- static iscsibinding interface index 392
- staticsafe containers
 - storing products in 465
 - transporting products in 465
- stopping
 - FCIP instances 298
- symbols in text xii
- symbols on equipment xiii

T

- tacacs-server host [34](#)
- tacacs-server key [36](#)
- tacacs-server timeout [37](#)
- tacas-server key [36](#)
- Taiwanese Notice [462](#)
- technical support, HP [xv](#)
- text symbols [xii](#)
- tools
 - conductive field service type [466](#)
- transparent SCSI routing
 - clear static mappings [274](#)
 - show static mappings [383](#)
- troubleshooting
 - displaying debug information [143](#)
 - displays
 - IP packet trace [228](#)
 - enabling iSCSI trace facilities [201](#)
 - iSCSI connections [201](#)

U

- username password [38](#)

V

- verify software [419](#)
- vlan [427](#)
- VLAN Commands [423](#)
- vtp domain [428](#)
- vtp mode [430](#)

W

- warning
 - rack stability [xiv](#)
 - symbols on equipment [xiii](#)
- websites
 - HP storage [xv](#)
- Wizard Commands [433](#)
- wizards
 - setup fcip [362](#)
- wrist straps
 - specifications [466](#)
 - using [466](#)